Internet & Jurisdiction Global Status Report 2019

Svantesson, Dan Jerker B

INTERNET & JURISDICTION

GLOBAL STATUS REPORT **2019**

KEY FINDINGS

AUTHOR: PROF. DAN JERKER B. SVANTESSON

INTERNET & JURISDICTION POLICY NETWORK

This Report was commissioned by the Secretariat of the Internet & Jurisdiction Policy Network and authored by Professor Dr. Dan Jerker B. Svantesson.

The Internet & Jurisdiction Global Status Report 2019, 1st Edition, is published by the Secretariat of the Internet & Jurisdiction Policy Network.

The author of this Report made a best effort to map the current ecosystem and trends based on desk-research, as well as stakeholder surveys and interviews. The completeness of information can however not be guaranteed, as this Report constitutes a first global baseline on the state of jurisdiction on the internet. Moreover, the analysis of the author does not necessarily reflect the view of the Secretariat of the Internet & Jurisdiction Policy Network, of stakeholders engaged in the Internet & Jurisdiction Policy Network, or of the financial supporters of the Report.

Internet & Jurisdiction Policy Network - Paris, France

The Secretariat of the Internet & Jurisdiction Policy Network is grateful for the financial and institutional support of the following entities that have enabled the production of the Report:

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

On behalf of Federal Ministry for Economic Cooperation and Development

Ministry of Foreign Affairs of Denmark

Republic of Estonia Ministry of Foreign Affairs

European Commission

REPORT CITATION

Internet & Jurisdiction Policy Network (2019). Internet & Jurisdiction Global Status Report 2019.

FOREWORDS

BERTRAND DE LA CHAPELLE and PAUL FEHLINGER
Executive Director and Deputy Executive Director
Internet & Jurisdiction Policy Network

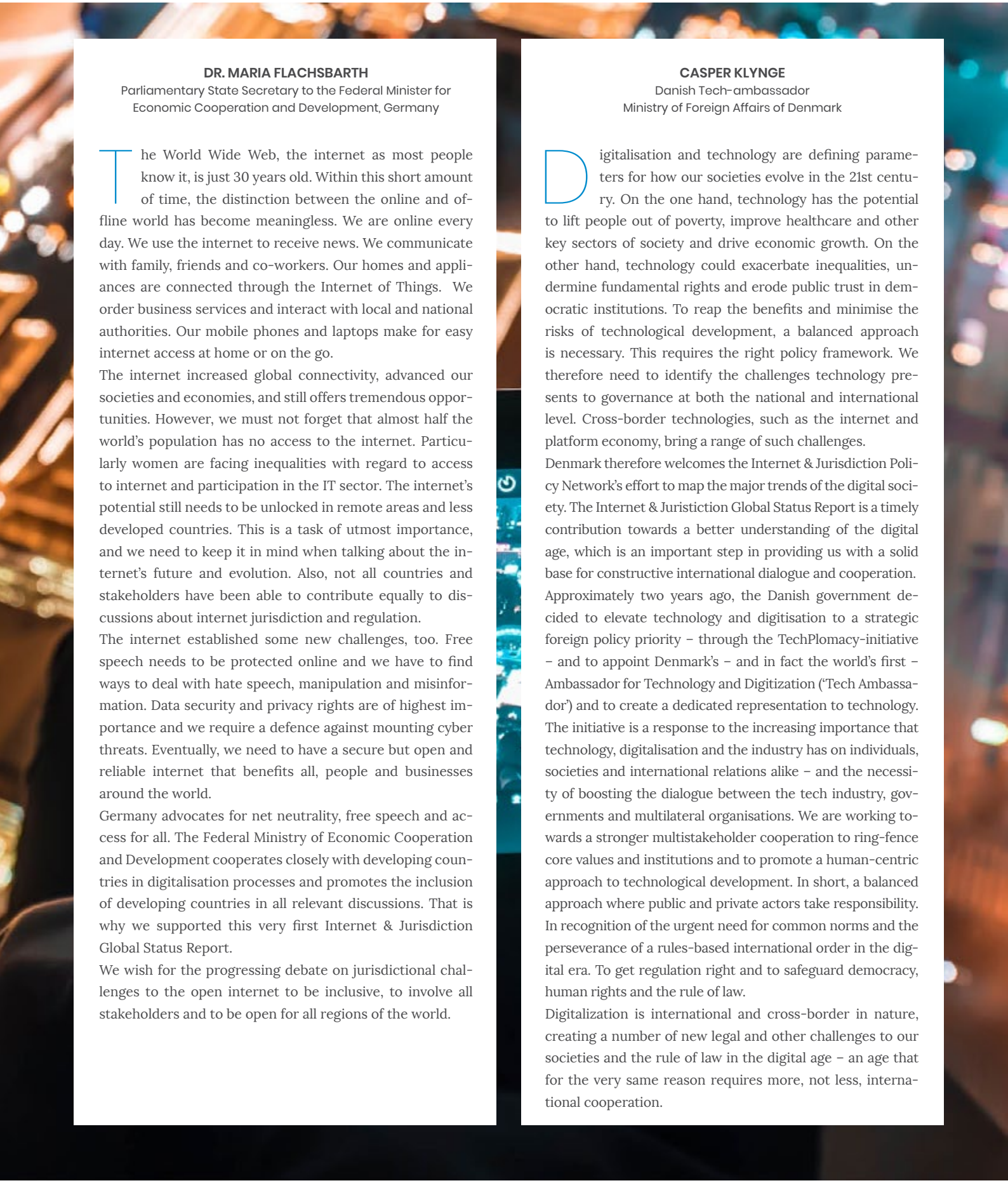
How to handle the coexistence of heterogeneous laws on the cross- border internet is one of the greatest policy challenges of the digital 21st century. Yet, scalable and coherent policy solutions cannot be developed without a comprehensive understanding of a highly complex and dynamic ecosystem comprised of multiple actors, initiatives and trends across the policy silos of digital economy, human rights and security. This was a clear call by over 200 key stakeholders from 40 countries at the 2nd Global Conference of the Internet & Jurisdiction Policy Network in 2018. However, even decades after the rise of the commercial internet, such consolidated data did not yet exist. To provide this indispensable mapping and analysis, the Secretariat of the Internet & Jurisdiction Policy Network thus decided to launch the world's first Internet & Jurisdiction Global Status Report.

Drawing on the unique expertise of key stakeholders engaged in the policy development work in the Internet & Jurisdiction Policy Network, this inaugural edition of the Global Status Report provides a first snapshot and baseline. It should be understood as a foundational dataset that will allow us to collectively proceed and fill in the gaps in future global and regional editions. For this ambitious and crucial endeavour, we invite all stakeholders to contribute their knowledge and share their data.

Clarifying how existing national laws apply in cyberspace and developing new balanced frameworks to address abuses, enable the digital economy and protect human rights will determine the shape of the emerging digital society for future generations. To preserve the open, cross-border nature of the internet, policy coherence and legal interoperability between multiple regimes need to be established. This requires communication, coordination and, ultimately, cooperation among all stakeholders.

Yet, sound policy-making must be based on evidence and reliable data. Policy coherence on a transnational basis can only be achieved through a shared understanding of the issues at stake and awareness of the various initiatives. The availability of this comprehensive overview and analysis of trends and initiatives will translate the highly complex and often technical nature of substantive issues for decision makers. This Report represents the first step of an ongoing effort by the Secretariat of the Internet & Jurisdiction Policy Network to make this essential information accessible to all stakeholders, to help them to collectively address some of the most pressing global challenges of our times.

We are delighted that the inaugural Internet & Jurisdiction Global Status Report will be launched on the occasion of the 3rd Global Conference of the Internet & Jurisdiction Policy Network. We would like to express our gratitude to the pioneers of this new global effort to foster policy coherence through capacity building and evidence-based policy innovation: the stakeholders in the Internet & Jurisdiction Policy Network, the author, Professor Dan Svantesson, as well as Germany, Denmark, Estonia and the European Commission, who are making this essential effort possible.



DR. MARIA FLACHSBARTH
Parliamentary State Secretary to the Federal Minister for Economic Cooperation and Development, Germany

The World Wide Web, the internet as most people know it, is just 30 years old. Within this short amount of time, the distinction between the online and offline world has become meaningless. We are online every day. We use the internet to receive news. We communicate with family, friends and co-workers. Our homes and appliances are connected through the Internet of Things. We order business services and interact with local and national authorities. Our mobile phones and laptops make for easy internet access at home or on the go.

The internet increased global connectivity, advanced our societies and economies, and still offers tremendous opportunities. However, we must not forget that almost half the world's population has no access to the internet. Particularly women are facing inequalities with regard to access to internet and participation in the IT sector. The internet's potential still needs to be unlocked in remote areas and less developed countries. This is a task of utmost importance, and we need to keep it in mind when talking about the internet's future and evolution. Also, not all countries and stakeholders have been able to contribute equally to discussions about internet jurisdiction and regulation.

The internet established some new challenges, too. Free speech needs to be protected online and we have to find ways to deal with hate speech, manipulation and misinformation. Data security and privacy rights are of highest importance and we require a defence against mounting cyber threats. Eventually, we need to have a secure but open and reliable internet that benefits all, people and businesses around the world.

Germany advocates for net neutrality, free speech and access for all. The Federal Ministry of Economic Cooperation and Development cooperates closely with developing countries in digitalisation processes and promotes the inclusion of developing countries in all relevant discussions. That is why we supported this very first Internet & Jurisdiction Global Status Report.

We wish for the progressing debate on jurisdictional challenges to the open internet to be inclusive, to involve all stakeholders and to be open for all regions of the world.

CASPER KLYNGE
Danish Tech-ambassador
Ministry of Foreign Affairs of Denmark

Digitalisation and technology are defining parameters for how our societies evolve in the 21st century. On the one hand, technology has the potential to lift people out of poverty, improve healthcare and other key sectors of society and drive economic growth. On the other hand, technology could exacerbate inequalities, undermine fundamental rights and erode public trust in democratic institutions. To reap the benefits and minimise the risks of technological development, a balanced approach is necessary. This requires the right policy framework. We therefore need to identify the challenges technology presents to governance at both the national and international level. Cross-border technologies, such as the internet and platform economy, bring a range of such challenges.

Denmark therefore welcomes the Internet & Jurisdiction Policy Network's effort to map the major trends of the digital society. The Internet & Juristiction Global Status Report is a timely contribution towards a better understanding of the digital age, which is an important step in providing us with a solid base for constructive international dialogue and cooperation.

Approximately two years ago, the Danish government decided to elevate technology and digitisation to a strategic foreign policy priority – through the TechPlomacy-initiative – and to appoint Denmark's – and in fact the world's first – Ambassador for Technology and Digitization ("Tech Ambassador") and to create a dedicated representation to technology. The initiative is a response to the increasing importance that technology, digitalisation and the industry has on individuals, societies and international relations alike – and the necessity of boosting the dialogue between the tech industry, governments and multilateral organisations. We are working towards a stronger multistakeholder cooperation to ring-fence core values and institutions and to promote a human-centric approach to technological development. In short, a balanced approach where public and private actors take responsibility. In recognition of the urgent need for common norms and the perseverance of a rules-based international order in the digital era. To get regulation right and to safeguard democracy, human rights and the rule of law.

Digitalization is international and cross-border in nature, creating a number of new legal and other challenges to our societies and the rule of law in the digital age – an age that for the very same reason requires more, not less, international cooperation.

HELI TIIRMAA-KLAAR
Ambassador at Large for Cyber Diplomacy,
Ministry of Foreign Affairs of Estonia

In 2018, the world reached an important milestone as more than 50% of its population had gained access to the internet. As demonstrated in the Internet & Jurisdiction Global Status Report, the internet has already revolutionized how people, businesses and governments interact. The multistakeholder governance model of the internet has provided a platform for enormous economic development and political progress globally. In order to continue this progress, it is critical that the accountable multistakeholder model of the internet will be maintained even if the growing interdependence on cyberspace seems to be creating unprecedented challenges. Although for many states, open, free and accessible cyberspace is part of their democratic identity, for some, internet governance may seem to be yet another tool for executing state control.

Estonia has always supported the open and interoperable internet. Non-discriminatory access to and accessibility of the internet are fundamentally important for enabling and promoting the right to freedom of expression, assembly and association. Access to independent media sources, social media platforms and a free Internet has become an integral part of good governance and a democratic society. While it should be clear that the existing international law applies to cyberspace, there is a need to further develop and implement norms of responsible state behaviour in this dynamic field. This evidently requires communication, coordination and cooperation among all stakeholders.

The Internet & Juristiction Global Status Report focuses on the overarching and topical trends as well as the legal and technical approaches and creates links between different global and regional initiatives. One of the incentives for this Report was to enable better access to relevant information, particularly the existing laws and their application. However, there still is a clear need for a meaningful coordination between multiple actors in the field and the existing initiatives.

The Report provides a comprehensive overview and documentation of the past, current and emerging trends. It also contributes to the global discussion on possible solutions for the major cross-border legal policy challenges. As a co-sponsor of the Report, Estonia is hoping to create bridges between the different initiatives and jurisdictions. We are certain that this Report will contribute to better coordination among different stakeholders for developing and protecting an interoperable and secure internetfor the global multistakeholder community.

PEARSE O'DONOHUE
Director for Future Networks
DG CONNECT, European Commission

The internet has already been in our lives for decades. It is now a critical means for transformation of our economy and society, and its importance will continue to grow. So it is our responsibility to ensure that the internet remains a human-centric, safe and trusted environment.

The EU's Digital Single Market strategy has achieved a lot in this respect. It has given European citizens, businesses, and public administrations new working and living opportunities in a safe and inclusive way, providing fair access to digital goods, content and services. Digital trust has been enhanced through the application of the General Data Protection Regulation, or the improvement of EU's resilience to cyber-incidents through a new Cybersecurity framework. With the DSM, the EU has provided concrete and tangible benefits to European citizens, but it has also taken a leading role in setting reference policy standards for the digital era.

The internet is, of course, a global phenomenon, and it is our ambition to drive the global policy debate on the internet with our partners and all stakeholders who share our values, as part of the multistakeholder approach to internet governance. This debate, which has traditionally focused on core internet infrastructures, needs to be broadened to cover issues such as the governance of Artificial Intelligence, the free flow of data or trust on the internet. Jurisdictional issues such as liability in case of services offered over the internet, the choice of law in case of dispute or the recognition of national laws and their enforcement, are also important. In addressing these issues, we must not allow accusations of protectionism to deflect us from maintaining a high level of protection of the individual.

The Internet & Jurisdiction Global Status Report 2019 offers a useful overview of the overarching trends affecting the cross-border nature of the internet. We welcome the effort of tracking legislative initiatives globally, soft law measures and best practices on the internet. This mapping exercise will certainly enrich the internet governance debate and stimulate the multistakeholder community in finding solutions to online jurisdictional problems. This is an important discussion to have if we want to maintain one global internet.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

This Report was commissioned by the Secretariat of the Internet & Jurisdiction Policy Network.

The production of this Report was enabled by financial support provided by the German Corporation for International Cooperation (GIZ) on behalf of the German Federal Ministry for Economic Cooperation and Development (BMZ), the Ministry of Foreign Affairs of Denmark, the Ministry of Foreign Affairs of Estonia and institutional support was provided by the European Commission, Directorate-General for Communications Networks, Content and Technology (DG CONNECT).

AUTHORSHIP TEAM:

AUTHOR:
Professor Dr. Dan Jerker B. Svantesson
Bond University
Gold Coast
Australia

RESEARCH AND
INTERVIEW ASSISTANCE:
Rebecca Azzopardi
Ph.D. Candidate
Bond University
Gold Coast
Australia

PROJECT COORDINATION:

Martin Hullin
Head of Operations and Partnerships
Secretariat of the Internet & Jurisdiction Policy Network

PROJECT TEAM:

Bertrand de la Chapelle,
Executive Director
Secretariat of the Internet & Jurisdiction Policy Network

Paul Fehlinger
Deputy Executive Director
Secretariat of the Internet & Jurisdiction Policy Network

Xavier Guyot de Camy
Policy Manager
Secretariat of the Internet & Jurisdiction Policy Network

Ajith Francis
Policy Officer
Secretariat of the Internet & Jurisdiction Policy Network

PRODUCTION:

Secretariat of the Internet & Jurisdiction Policy Network, Paris, France

EDITING:

Amar Toor, Paris, France

DESIGN AND LAYOUT:

Formas do Possível - Creative Studio, Lisbon, Portugal

The Secretariat greatly appreciates the time and contribution of all participating survey respondents and interviewees. Without their valuable insights, this report could not have been produced.

Waiswa Abudu Sallam
Head Legal Affairs
Communications Commission
Uganda

Benedict Addis
Chair
Registrar of Last Resort (RoLR)
UK

Fiona Alexander
Associate Administrator for
International Affairs
Department of Commerce
National Telecommunications and
Information Administration (NTIA)
USA

Chinmayi Arun
Assistant Professor of Law
National Law University Delhi
India

Karen Audcent
Senior Counsel
Department of Justice
Canada

Kerry Ann Barrett
Cybersecurity Policy Specialist
Organization of American States (OAS)
USA

Elizabeth Behsudi
Former General Counsel
Public Interest Registry (PIR)
USA

Tijani Ben Jemaa
Executive Director
Fédération Méditerranéenne des
Associations d'Internet (FMAI)
Tunisia

Eduardo Bertoni
Director
National Access to Public Information
Agency
Argentina

Theo Bertram
Public Policy Manager
Google
USA

Ellen Blackler
Vice President
Global Public Policy
The Walt Disney Company
USA

Marko Bošnjak
Judge
European Court of Human Rights (ECHR)
France

Maarten Botterman
Board Director
The Internet Corporation for Assigned
Names and Numbers (ICANN)
Netherlands

Andrew Bridges
Partner
Fenwick & West LLP
USA

Lisl Brunner
Director
Global Public Policy
AT&T
USA

Jordan Carter
Chief Executive
InternetNZ
New Zealand

Mark Carvell
International Online Policy Senior Adviser
Department for Digital
Culture
Media and Sport (DCMS)
UK

Angelica Chinchilla-Medina
Director
Ministry of Science
Technology and Telecommunications,
Costa Rica

Jose Clastornik
Executive Director
AGESIC - National eGovernment and
Information Society Agency
Office of the President of Uruguay

Alexander Corbeil
Research Advisor
Public Safety Canada
Canada

Jennifer Daskal
Associate Professor
American University
Washington College of Law
USA

Bertrand De la Chapelle
Executive Director
Secretariat of the Internet & Jurisdiction
Policy Network
France

Jacques De Werra
Professor
University of Geneva
Switzerland

Agustina Del Campo
Director
Center for Studies on Freedom of
Expression and Access to Information
(CELE)
Argentina

Steven Delbianco
President
NetChoice
USA

Fernanda Domingos
Federal Prosecutor
Federal Prosecution Service
Brazil

Brendan Eiffe
Head of Mutual Legal Assistance
DivisionDepartment of Justice
and Equality
Ireland

Paul Fehlinger
Deputy Executive Director
Secretariat of the Internet & Jurisdiction
Policy Network
France

Benedicto Fonseca Filho
Ambassador
Ministry of Foreign Affairs
Brazil

Jothan Frakes
Executive Director
The Domain Name Association
USA

Eric Freyssinet
Chief Digital Strategy Officer
Gendarmerie nationale
France

Giancarlo Frosio
Senior Lecturer
University of Strasbourg
CEIPI
France

Lise Fuhr
Director General
European Telecommunications Network
Operators' Association (ETNO)
Belgium

Chawki Gaddes
Président
Instance Nationale de Protection des Données Personnelles (INPDP)
Tunisia

Michael Geist
Canada Research Chair in Internet and E-commerce Law
University of Ottawa
Canada

Jan Gerlach
Senior Public Policy Manager
Wikimedia Foundation
USA

Grace Githaiga
Co-convenor
Kenya ICT Action Network (KICTANet)
Kenya

Hartmut Glaser
Executive Secretary
Brazilian Internet Steering Committee/CGI.br
Brazil

Tonei Glavinic
Director of Operations
Dangerous Speech Project
Spain

Joaquín Gonzalez-Casanova
Director General for International Affairs
Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales
Mexico

Nicole Gregory
Head Data and Online Harms,
Foreign & Commonwealth Office
UK

Devesh Gupta
Manager
Reliance Industries Limited (RIL)
India

Hiroki Habuka
Deputy Director, Digital Economy Division
Ministry of Economy, Trade and Industry (METI)
Japan

Statton Hammock
Vice-President
MarkMonitor
USA

Byron Holland
President and CEO
Canadian Internet Registration Authority (CIRA)
Canada

Daniel Holznagel
Legal Officer
Federal Ministry of Justice and Consumer Protection
Germany

Martin Husovec
Assistant Professor
Tilburg University
Netherlands

Manal Ismail
Executive Director
International Technical Coordination
National Telecom Regulatory Authority (NTRA)
Egypt

Sunali Jayasuriya
Legal Officer
Information and Communication Technology (ICT) Agency
Sri Lanka

Tarek Kamel
Senior Advisor,
The Internet Corporation for Assigned Names and Numbers (ICANN)
Egypt

Seb Kay
Policy Adviser
Foreign & Commonwealth Office
UK

Daphne Keller
Director of Intermediary Liability
Stanford Law School Center for Internet and Society
USA

Gail Kent
Global Public Policy Lead on Law Enforcement and Surveillance
Facebook
USA

Tshoganetso Kepaletswe
Chief Technology Officer
Communications Regulatory Authority
Botswana

Matthias Kettemann
Co-Head
Research Focus Internet & Society
University of Frankfurt/Main
Germany

Gayatri Khandhadai
Asia Policy Regional Coordinator
Association for Progressive Communications (APC)
India

Jan Kleijssen
Director of Information Society and Action against Crime, Council of Europe
France

Wolfgang Kleinwächter
Professor
Global Commission on the Stability in Cyberspace (GCSC)
Germany

Casper Klynge
Tech Ambassador
Ministry of Foreign Affairs
Denmark

Dominique Lazanski
Director
Public Policy and International Relations
GSMA
UK

Emmanuelle Legrand,
Legal and Policy Officer
European Commission (EC)
Belgium

Lim May-Ann
Executive Director
Asia Cloud Computing Association and Managing Director, TRPC Pte Ltd
Singapore

Rebecca Mackinnon
Director
Ranking Digital Rights
New America
USA

Giacomo Mazzone
Head of Institutional Relations
European Broadcasting Union (EBU)
Switzerland

Corynne McSherry
Legal Director
Electronic Frontier Foundation (EFF)
USA

Francesca Musiani
Associate Research Professor (eq.)
Centre Nationale de la Recherche Scientifique (CNRS)
France

Victoria Nash
Senior Policy Fellow
University of Oxford
UK

Gonzalo Navarro
Chief Executive Officer
Latin American Internet Association (ALAI)
Chile

Paul Nemitz
Principal Adviser
European Commission (EC)
Belgium

Michele Neylon
Chief Executive Officer
Blacknight Internet Solutions Ltd
Ireland

Gregory Nojeim
Director
Freedom
Security & Technology Project
Center for Democracy & Technology (CDT)
USA

Elliot Noss
Chief Executive Officer
Tucows
Canada

Seun Ojedeji
Chief Network Engineer
Federal University Oye-Ekiti
Nigeria

Elena Perotti
Executive Director Public Affairs
and Media Policy
World Association of Newspapers
and News Publishers (WAN-IFRA)
France

Nick Pickles
Senior Public Policy Strategist
Twitter
USA

Jason Pielemeier
Policy Director
Global Network Initiative (GNI)
USA

Marc Porret
Legal and Criminal Justice Coordinator
United Nations Counter-Terrorism
Committee Executive Directorate
(UNCTED)
USA

Frederic Potier
National Delegate
Délégation Interministérielle à la Lutte
Contre le Racisme l'Antisémitisme et la
Haine anti-LGBT (DILCRAH)
France

Rod Rasmussen
Principal
R2 Cyber
USA

Chris Riley
Director
Public Policy
Mozilla
USA

Jorge Rodríguez-Zapata
Justice
Supreme Court
Spain

Elettra Ronchi
Head of Unit
Organization for Economic Co-operation
and Development (OECD)
France

Kostas Rossoglou
Head of EU Public Policy
Yelp
Belgium

Alexandre Roure
Senior Manager
Public Policy, Computer & Communication
Industry Associations (CCIA)
USA

Nicolás Schubert
Digital Economy Coordinator
General Directorate of International
Economic Affairs
Ministry of Foreign Affairs
Chile

Jörg Schweiger
Chief Executive Officer
DENIC eG
Germany

Alissa Starzak
Head of Public Policy
Cloudflare
USA

Christoph Steck
Director
Public Policy
Telefonica
Spain

Blair Stewart
Assistant Commissioner
Office of the Privacy Commissioner
New Zealand

Peter Swire
Professor
Georgia Tech Scheller College of Business
USA

Takahiko Toyama
Director for Information Policy Planning
Ministry of Economy, Trade and Industry
(METI)
Japan

Lee Tuthill
Counsellor
World Trade Organisation (WTO)
Switzerland

Kimmo Ulkuniemi
Chief Superintendent
National Police Board
Finland

Peter Van Roste
General Manager
CENTR
Belgium

Mark Villiger
Retired Judge
Formerly Section President
European Court of Human Rights (ECtHR)
France

Ian Walden
Professor of Information and
Communications Law
Queen Mary University of London
UK

Rolf H. Weber
Professor of International Business Law
University of Zurich
Switzerland

Paul Wilson
Director General
Asia-Pacific Network Information Center
(APNIC)
Australia

Shinichi Yokohama
Chief Information Security Officer
Nippon Telegraph & Telephone (NTT)
Japan

Nicolo Zingales
Lecturer
Sussex University
UK

EXECUTIVE SUMMARY

The internet plays a central role in the lives of billions of people, facilitating cross-border contacts, trade, and the sharing of ideas and knowledge. Much like the 'tipping points' that scientists have pointed to in the context of climate change, Internet & Jurisdiction Global Status Report 2019 – the first of its kind – shows that if developments continue along their current course, we will soon reach a point at which the cross-border internet as we know it ceases to exist – and from which attempts at a reversal are potentially futile.[1] The Global Internet & Jurisdiction Global Status Report 2019 launched an unprecedented structured global mapping process of the state of jurisdiction on the internet at global and regional levels.

This Report combines detailed desk research with a pioneering data collection from already over 100 key stakeholders of the Internet & Jurisdiction Policy Network: states, Internet companies, technical operators, civil society, academia and international organizations.

Almost 80% of stakeholders think that there is not sufficient international coordination and coherence to address cross-border legal challenges on the Internet. This is a grave concern for the international community as the overwhelming majority of the surveyed stakeholders is convinced that cross-border legal challenges on the internet will only become more acute in the next three years. More than half of the stakeholders think that we do not yet have the right frameworks and standards in place to address cross-border legal challenges on the internet.

According to stakeholders, cross-border legal challenges on the internet are increasingly acute because of three factors:

1. The world is increasingly becoming interconnected through the internet, thereby increasing diversity online;
2. The internet is deeply affecting societies and economies, meaning that the stakes are high; and
3. Nation states, with different visions, are seeking to increase their control over the internet, primarily through national tools rather than transnational cooperation and coordination.

The regulatory environment online is characterized by potentially competing or conflicting policies and court decisions in the absence of clear-cut standards. The resulting complexity may be detrimental on numerous levels because it:

1. Prevents actors from efficiently addressing abuses online;
2. Creates high levels of legal uncertainty in cyberspace;
3. Risks resulting in competing assertions of jurisdiction and unwanted fragmentation of online spaces;
4. Creates situations where compliance with one state's law unavoidably results in a direct violation of another state's law;
5. Generates distrust amongst internet users who cannot know what laws apply to their online activities; and
6. Hampers digital innovation and growth of the internet economy, especially in developing countries and for SMEs.

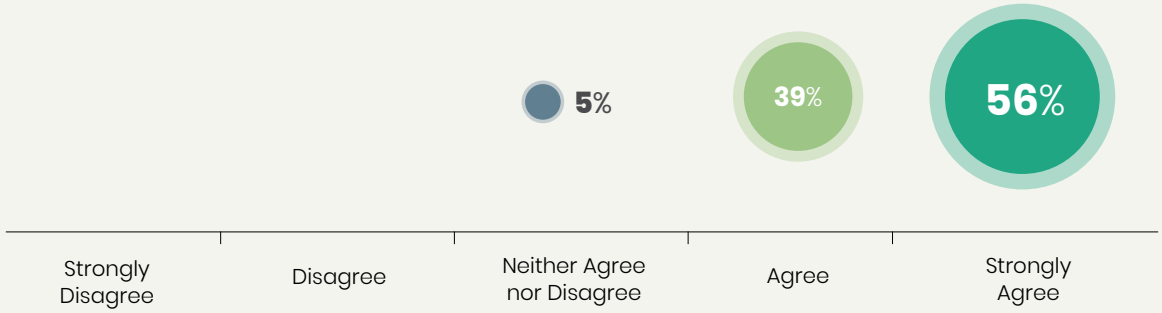
AT A GLANCE...

- Cross-border legal challenges on the internet are increasingly acute.
- Normative plurality in cyberspace is rising.
- The risk of a harmful legal arms race is very high.
- Important human rights are at stake.
- Cyberspace risks being fragmented along national borders.
- Online abuses risk not being addressed efficiently in the absence of cooperation.
- Developing countries and SMEs are facing significant regulatory barriers.
- The governance ecosystem is characterised by competing agendas and values.
- The regulatory complexity is increasing, leading to legal uncertainty.
- Central legal concepts are outdated and prevent progress.
- Private actors are increasingly performing quasi-public regulatory and judicial roles.
- Stakeholders call for appropriate institutions, frameworks and policy standards.
- Stakeholders call for greater international coordination.
- Stakeholders call for inclusiveness and capacity building.
- Stakeholders stress the value of multistakeholderism.

1. It is possible to imagine each of these tipping points being reached also on a smaller scale within specific countries or within specific online platforms. However, the focus here is on the current internet as a whole.

INFOGRAPHIC 1

Will cross-border legal challenges on the internet become increasingly acute in the next three years?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

The surveys and interviews with key stakeholders reveal several important trends, including:

1. The constant flux of digital innovation and transnational nature of the internet makes it increasingly challenging to address online abuses with traditional national legal tools;
2. Regulatory initiatives by both public and private actors proliferate now at unprecedented speeds around the world;
3. Stakeholders lose track of the multitude of laws and initiatives around the world; capacity building and consolidated, accessible data on trends are needed to make informed decisions and ensure policy coherence;
4. Extraterritorial assertions of national jurisdiction online are on the rise; and
5. There is a clear need for re-examining and more clearly defining the roles of intermediaries.

The Report points to several key obstacles to addressing the cross-border legal issues online:

1. There is no common agreement on substantive values;
2 There is no common understanding of key concepts and vernacular;
3. Trust risks being replaced by distrust, and collaboration by the rule of the strongest;
4. In some regions, stakeholders feel they are subjected online to rules that were developed without them in other parts of the world;

5. Much of what has been done to date has involved trying to solve global problems through a national lens;
6. Urgency-driven unilateral actions tend to prevent a consistent and coordinated approach to regulatory issues; and
7. There are practical issues such as a lacking access to relevant information due to language and cultural barriers, as well as information overload.

There is much that needs to change in order to overcome the cross-border legal challenges facing the online environment. The stakeholders specifically pointed to the need for:

1. More cooperation;
2. Inclusiveness and capacity building;
3. Engaging, in a coordinated manner, with both substantive and procedural standards;
4. Considering the respective roles of the private and the public sector;
5. Transparency and accountability;
6. Solutions pursued on an issue-by-issue basis, or as clusters of issues;
7. Continued, or even expanded, adherence to multistakeholderism; and
8. A recognition that no state, company or organization can address these issues on its own, and that the ecosystem simply cannot afford *not* to collaborate.

In the end, stakeholders stressed that the issue of jurisdiction on the internet is not just a matter of finding the 'right' legal principles. Rather, it is fundamentally about developing the frameworks and standards that will shape the future of the digital society that we collectively want - for us and the generations after us.

Method

It is daunting to embark on a mapping and analysis exercise aimed at facilitating a comprehensive understanding of a highly complex and dynamic ecosystem – one comprised of multiple actors, initiatives and trends across the policy silos of digital economy, human rights and security. Such an undertaking presents several challenges. Most obvious is the difficulty in facilitating a sufficiently deep understanding of the complex issues associated with the coexistence of heterogeneous laws on the cross-border internet – one of the greatest policy challenges of the 21st century.

Furthermore, there are challenges associated with seeking to fully understand, and represent fairly, the diverse views and multifaceted interests involved. Another considerable challenge is that of the so-called 'unknown unknowns'; with any research task involving great sectoral and geographical diversity comes a risk of missing something important without even realizing that it is missing.

An awareness of the mentioned challenges shaped the method of this report, and led to the consideration of a flexible, qualitative research design that enables an in-depth exploration of the research questions. To overcome the challenges cited above, this writing project has adopted a multifaceted research method incorporating an unprecedented and innovative large-scale collaborative contribution and review process. This process leveraged the combined expertise of the key stakeholders engaged in the Internet & Jurisdiction Policy Network through semi-structured interviews, peer review feedback and data collection procedures, combined with detailed and extensive desk research.

The desk-research

Desk research adopted conventional legal research methods and consisted primarily of a comprehensive study and analysis of relevant case law, legislation and other regulatory initiatives, as well as the literature – including books, journal articles, published conference papers and industry publications. This was supplemented with a detailed study of a variety of valuable reports and other materials from a range of bodies over recent years.

The desk research benefited greatly from the Internet & Jurisdiction Policy Network's wide-ranging collection of relevant developments available in the I&J Retrospect Database.[2] The Retrospect Database is the flagship, open-access publication of the Internet & Jurisdiction Policy Network, documenting policy developments, judicial decisions, international agreements and other cases that reflect jurisdictional tensions on the cross-border internet. This important collection provided up-to-date insights into current major trends, attitudes, developments and initiatives.

The materials contained in the Retrospect Database also provided important insights into current legal and technical approaches to solutions, as well as in relation to what this Report defines as overarching 'meta-trends'.

Stakeholder survey

The first method for gaining stakeholder input consisted of an online survey made up of 17 questions on a variety of topics relevant for the research questions. In considering how best to gather survey data to inform the research questions, great care was taken to design questions that may be answered by any of the relevant stakeholders. This ensured that all survey participants were exposed to the same set of questions.

The Internet & Jurisdiction Policy Network Secretariat identified survey participants representing all its stakeholder groups – i.e., academia, civil society, governments, international organizations, internet platforms and the technical community – and participants were specifically selected to guarantee geographical diversity. To that end, specific geographic regions were targeted to capture as much variation as is possible. Furthermore, the selection of the survey participants was purposive, in that they were specifically targeted based on their considerable expertise and knowledge. In total, input was received from 100 survey participants during a period from Autumn 2018 to Spring 2019. Participants provided their views in their personal capacities, rather than as representatives of any specific organization. Furthermore, input gained from the surveys has only been used without attribution.

---

2. Internet & Jurisdiction Policy Network. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect.

"The expert input gained from the survey was invaluable. Apart from bringing attention to major topical trends, approaches to solutions, overarching meta-trends and generally held concerns in the ecosystem, the survey results helped provide both context and a more nuanced understanding of the operating environments facing civil society, governments, international organizations, internet platforms and the technical community."

The expert input gained from the survey was invaluable. Apart from bringing attention to major topical trends, approaches to solutions, overarching meta-trends and generally held concerns in the ecosystem, the survey results helped provide both context and a more nuanced understanding of the operating environments facing civil society, governments, international organizations, internet platforms and the technical community.

Survey results are used throughout the Report to show, in figures, the concerns and attitudes of the Internet & Jurisdiction Policy Network's stakeholder ecosystem. In addition, the comments from surveyed experts are used to highlight particularly important arguments, observations and concerns.

Stakeholder interviews

Semi-structured interviews were organized across a broad range of stakeholders in order to complement the insights gained from the survey responses and desk research. As with the surveys, the Internet & Jurisdiction Policy Network Secretariat took care to ensure inclusiveness and diversity, with the selected interviewed experts representing academia, civil society, governments, international organizations, internet platforms and the technical community, with geographical diversity. These stakeholders were identified both from within and outside the Internet & Jurisdiction Policy Network.

Each interview lasted over 30 minutes, on average. The interviews were conducted in confidence and as such, were not recorded. Detailed notes were collated, however, and observations recorded in a structured manner facilitating cross-referencing and detailed analysis.

The semi-structured interviews allowed for considerable flexibility and catered for supplementary questions based on discussions with the interviewee. This – combined with the confidentiality guarantee – provided an environment in which interviewed experts could highlight matters important to them within the topics discussed. In many cases, the interviewees could also provide perspectives, insights and information that might otherwise have been unattainable by researchers. In this way, part of the purpose of the interviews was to reduce regional and topical gaps in the desk research. In total, 63 interviews were carried out from Autumn 2018 to Spring 2019. The interviewed experts provided their views in their personal capacities rather than as representatives of any specific organization. Furthermore, input gained from the interviews has only been used without attribution.

Like the comments made by surveyed experts, the interviewed experts' comments were vital and are used throughout the Report to highlight particularly important arguments, observations and concerns.

Stakeholder feedback

Apart from the surveys and interviews, stakeholder input was sought by sharing an advanced version of the report with contributors. The input gained from this review was tremendously valuable and has helped ensure the quality of this Report, particularly by minimizing regional and topical gaps.

Limitations of the study

A research study of this nature carries certain limitations. Despite the steps outlined above, the inevitable risk of

gaps must be acknowledged. The statistical relevance of exploratory research relying, in part, on a limited number of survey participants and interviewed experts should not be overstated. In addition, most forms of desk research may be accused of involving biases that are difficult to eliminate in full.

In light of the above, this Report represents a best-effort attempt at painting a broad-brushed, yet comprehensive, overview and documentation of past, current and emerging trends; relevant actors; and proposed solutions to the major cross-border legal policy challenges facing our connected society as of 1 January 2019. As such, it is a timely snapshot of the policy environment and creates a first baseline against which future studies may be undertaken.

Outlook

On the occasion of the 14th United Nations Internet Governance Forum, full versions of Chapters 3 (Topical Trends), 4 (Legal and technical approaches) and 5 (Relevant concept clusters) will be launched that will supplement the initial key findings in this edition. Stakeholders from around the world will be invited between June-October 2019 to contribute online to the global data collection and mapping effort, adding to the input from more than 100 key stakeholders from five continents who contributed to the present Key Findings of the first edition of the Internet & Jurisdiction Global Status Report 2019.

01

WHY A GLOBAL STATUS REPORT, AND WHAT IS AT STAKE?

—

EXPRESSION

SECURITY

ECONOMY

1.1

Responding to the call from the Internet & Jurisdiction Policy Network

The Internet & Jurisdiction Global Status Report 2019 is the first of its kind. It is produced in response to the urgent call of over 200 senior-level stakeholders from 40 countries at the 2nd Global Conference of the Internet & Jurisdiction Policy Network in Ottawa in February 2018.

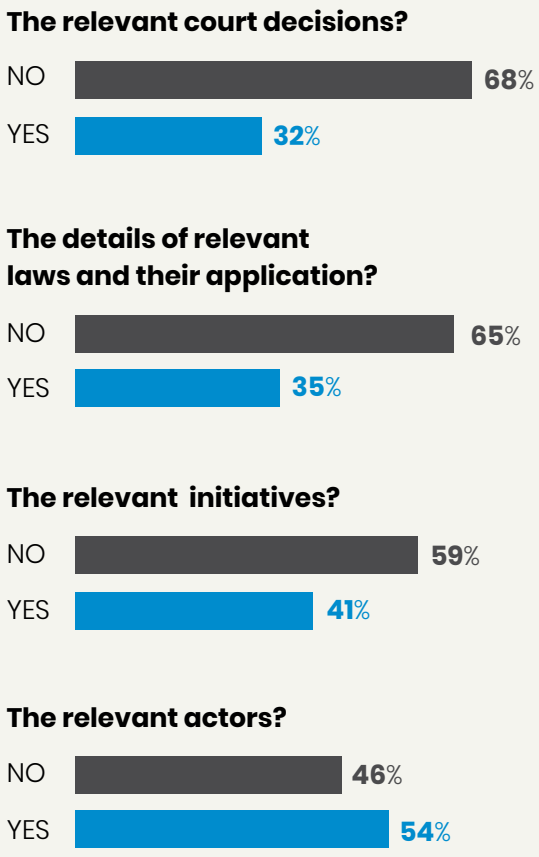
The primary aim of the Global Status Report is to provide a snapshot of the current landscape and to reflect the current thinking, concerns, trends and proposals of the Internet & Jurisdiction Policy Network's diverse stakeholders. Thus, the aim is to both provide an objective assessment of what this ecosystem of stakeholders faces today, and to anticipate relevant developments by, for example, highlighting overarching trends that will impact developments for the foreseeable future.

A secondary aim is for the Global Status Report to be a useful resource for capacity building, and for creating a greater understanding of the complicated issues involved – issues that stand to profoundly affect the entire ecosystem. To a degree, the Report may also provide a much-needed baseline for future studies of legal and regulatory trends at a global level.

Surveyed experts were asked whether they currently have easy access to enough information about the relevant actors, initiatives, laws and court decisions. While the survey highlighted some regional and sectoral differences, it also identified a clear need for better access to relevant information.

INFOGRAPHIC 2

On the topic of cross-border legal challenges on the internet, do you currently have easy access to enough information about:



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

As these results make clear, there is considerably greater access to sufficient information about relevant actors and initiatives, than to information about the details of relevant laws and their application, or to relevant court decisions. Stakeholders from non-OECD countries indicated a considerably lower degree of easy access to information about the relevant actors and initiatives, which suggests a need for capacity building and outreach to facilitate ongoing and future conversations.

When asked whether there is easy access to enough information about the details of relevant laws and their application, the answer was a resounding 'no' across regions and stakeholder groups, apart from academia. No less than 50 % of respondents from academia indicated that they have easy access to such information, implying that the problem is not an absence of information, but rather concerns the accessibility of such information. This can be partly explained by the fact that some information sits behind paywalls in databases that are commonly accessible to stakeholders in academia, but less so for other stakeholder groups. Yet there are also numerous free online databases that provide easy access to extensive information on the details of relevant laws and their application.[3] Ultimately, then, this aspect of the survey results highlights a need for capacity building.

In comments from surveyed and interviewed experts, it was clear that respondents were gaining access to relevant information, but in neither a consistent nor comprehensive manner. The lack of a single authoritative source, reliance on multiple (sectoral) newsletters, the lack of transparency and online access, the use of legal jargon, and information overload were all mentioned as concerns. The broad scope of the topic may be a factor, as well. As made clear in Chapter Three, which examines topical trends, cross-border legal challenges on the internet arise in such a diverse range of substantive areas that it is extremely onerous and challenging to stay up-to-date.

It is noteworthy that the surveyed experts made no specific reference to academic writings as a source of information, suggesting that the work of academics does not effectively reach the other stakeholder groups. There would be significant value in exploring options for improving this transfer of knowledge.

In enabling evidence-based policy innovation, the Report seeks to provide all stakeholders with the necessary information to develop frameworks and policy standards for the digital society and economy. It aims to give a comprehensive and regionally balanced overview and documentation of past, current and emerging trends, relevant actors and proposed solutions to the major cross-border legal policy challenges facing the connected society. In doing so, the Report accounts for the fact that the internet may be approached as: (a) a physical technical infrastructure (i.e., the hardware, routers, servers, computers, satellites, fiber optic cables, etc.); (b) a logical structure (i.e., the technical protocols that govern online interactions); and (c) a social construct made up of the available content and cyber activities.

The Report complements the ongoing policy development process facilitated by the Secretariat of the Internet & Jurisdiction Policy Network. Thus, it builds upon the findings and issues addressed in the three thematic Programs of the Internet & Jurisdiction Policy Network, namely:

1. Data & Jurisdiction Program;
2. Content & Jurisdiction Program;
3. Domains & Jurisdiction Program.

The Report's topical coverage has been selected, and is limited, by reference to the Internet & Jurisdiction Policy Network's focus on internet governance at the intersection of the three areas of digital economy, human rights, and cybersecurity. Therefore, the coverage is not limited to questions of internet jurisdiction *per se*, but rather encompasses a broad range of procedural and substantive law issues falling within the broad topic of cross-border legal challenges facing the internet.

In alignment with the Internet & Jurisdiction Policy Network's focus areas, the Report addresses neither cyberwar, nor cyber conflict more broadly. At the same time, it is not always possible to distinguish activities that fit within the field of cyber conflict from those that do not, the online environ-

> "The coverage is not limited to questions of internet jurisdiction per se, but rather encompasses a broad range of procedural and substantive law issues falling within the broad topic of cross-border legal challenges facing the internet."

3. Free Access to Law Movement. Retrieved from http://www.falm.info/members/current/.

ment. For example, cyber espionage is carried out for both military and economic purposes, and when it is directed at defense industries or critical infrastructure, distinguishing between military and non-military espionage may be virtually impossible; rather, such espionage activities are simultaneously military and non-military. Likewise, drawing a sharp line between national security information sharing and information sharing in the context of law enforcement is not always possible, either.

A significant number of stakeholders have called for a timely compendium of global activities. It is hoped that this Report – made possible by the strong support that the Internet & Jurisdiction Policy Network enjoys from its stakeholders – can meet that need and serve as a crucial instrument to help foster policy coherence across ongoing initiatives.

Thus, the Report stands to contribute to the mitigation of acute jurisdictional conflicts, to support the development of concrete operational solutions, and to preserve the benefits of the open, interoperable and cross-border internet.

1.2

Transnational as the new normal

The world consists of nearly 200 countries, some industrialized and some developing. All these countries have their own history, economy and cultures. They have different social structures, political systems and laws. Many are home to a diverse range of cultures, and some have a diverse range of laws. The people who populate these countries are of different ethnicities, and they speak different languages. They hold different values, religious beliefs and political opinions. Indeed, even where they hold the same values as important, they frequently take different views on how those shared values should be balanced in cases where they clash with one another. This incredible diversity stands in contrast to the fact that we all – so far – essentially share one internet.

During interviews carried out in support of the Report drafting, the European Union's General Data Protection Regulation (GDPR), introduced in 2018, was by far the most frequently mentioned legal initiative. Few, if any, previous legislative initiatives have gained a similar degree of international attention. So why is it that one can speak to people from anywhere in the world and find that they are not only aware, but have detailed knowledge, of the GDPR – a law issued by lawmakers in Europe, far away from countries such as Australia, Brazil, China and the Democratic Republic of Congo? When the European Union introduced its Data Protection Directive in the mid-1990s, it gained only limited and sectoral international attention. What then changed in the world to render the GDPR a virtually ubiquitous topic of discussion?

The answer is probably twofold. First, globalization has changed the world since the mid-1990s, and the ecosystem is now more alert to how the laws of one jurisdiction can impact people in other parts of the world. This is an inescapable consequence of increased interconnectedness. Further, states are now more frequently looking to other states when seeking to shape their own legal responses to the challenges that stakeholders face. The internet has strongly contributed to these developments. Second, there is now considerably greater recognition of the role that data – and therefore data privacy – play in our lives. This change, too, has been predominantly driven by the internet.

The GDPR is merely one of many laws that impact individuals beyond their original jurisdiction. In fact, most countries' laws have such an impact on some level. As many interviewed experts observed, this makes for an increasingly complex regulatory environment.

The observation that the online environment is largely transnational may seem like little more than a truism; but this trend has profound implications, giving rise to problems and affecting approaches to their solution. Several interviewed and surveyed experts noted that matters that were once determined domestically are now transnational in nature, necessitating a different mindset among decision makers on all levels. The stakes are high, and the diversity is great.

The importance of communication (including cross-border communication) is well-established; and no other medium can facilitate cross-border communication as fluidly as the in-

ternet. The online environment lends itself to the kind of cross-border communication that online communities in both industrialized and developing countries expect, and that can lead to cross-border disputes. Addressing transnational issues is therefore not optional, and the necessary internet jurisdiction rules must be able to cope with a high volume of disputes.

As an international environment, issues of internet regulation also require internationally oriented solutions; whether pursued on an international or domestic level, solutions must account for the international context in which they will operate. Both useful and harmful approaches are likely to have cross-border implications and may spread internationally. Kant's 'categorical imperative' comes to mind, prompting the pursuit of universal solutions.

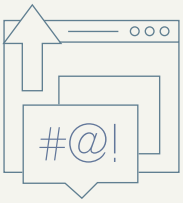
Unfortunately, the international climate has recently changed. There is a significant move away from international collaborative efforts and common goals, as more states adopt inward-looking policies and put their own immediate interests first. Trust is being replaced by distrust, collaboration by the rule of the strongest. This political trend represents a substantial obstacle for the effective coordination of internet regulation. However, it remains an inescapable fact that cross-border legal challenges on the internet can only be addressed through international collaborative efforts and the pursuit of common goals; no state, company or organization can do this on its own, and the ecosystem simply cannot afford not to collaborate.

> "Trust is being replaced by distrust, collaboration by the rule of the strongest."

1.3

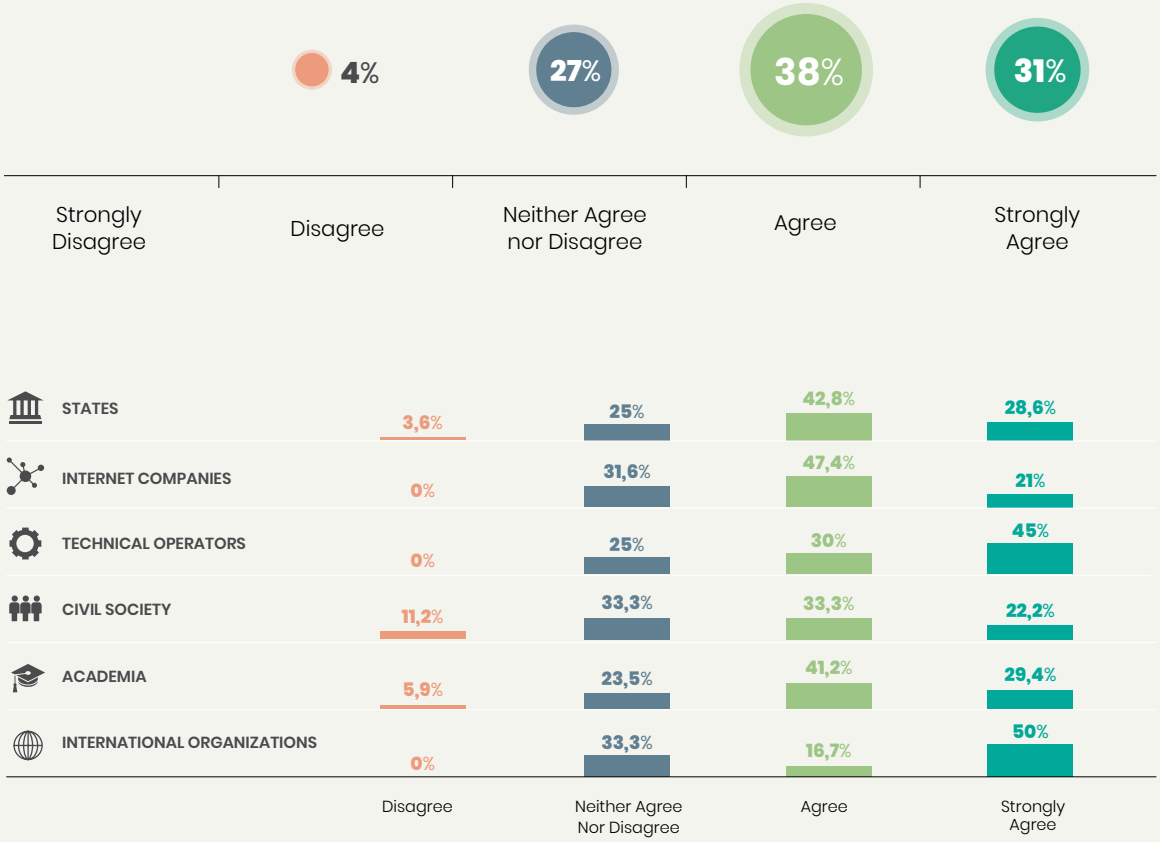
Growing concern over abuses

There is a general feeling among the Internet & Jurisdiction Policy Network's stakeholders that online abuse is increasing. A clear majority – 69% of surveyed experts – either 'agreed' or 'strongly agreed' that online abuses (e.g., in the form of hate speech, harassment, hacking, privacy violations, or fraud) are increasing. 27% 'neither agreed nor disagreed', and only 4% 'disagreed' or 'strongly disagreed'.

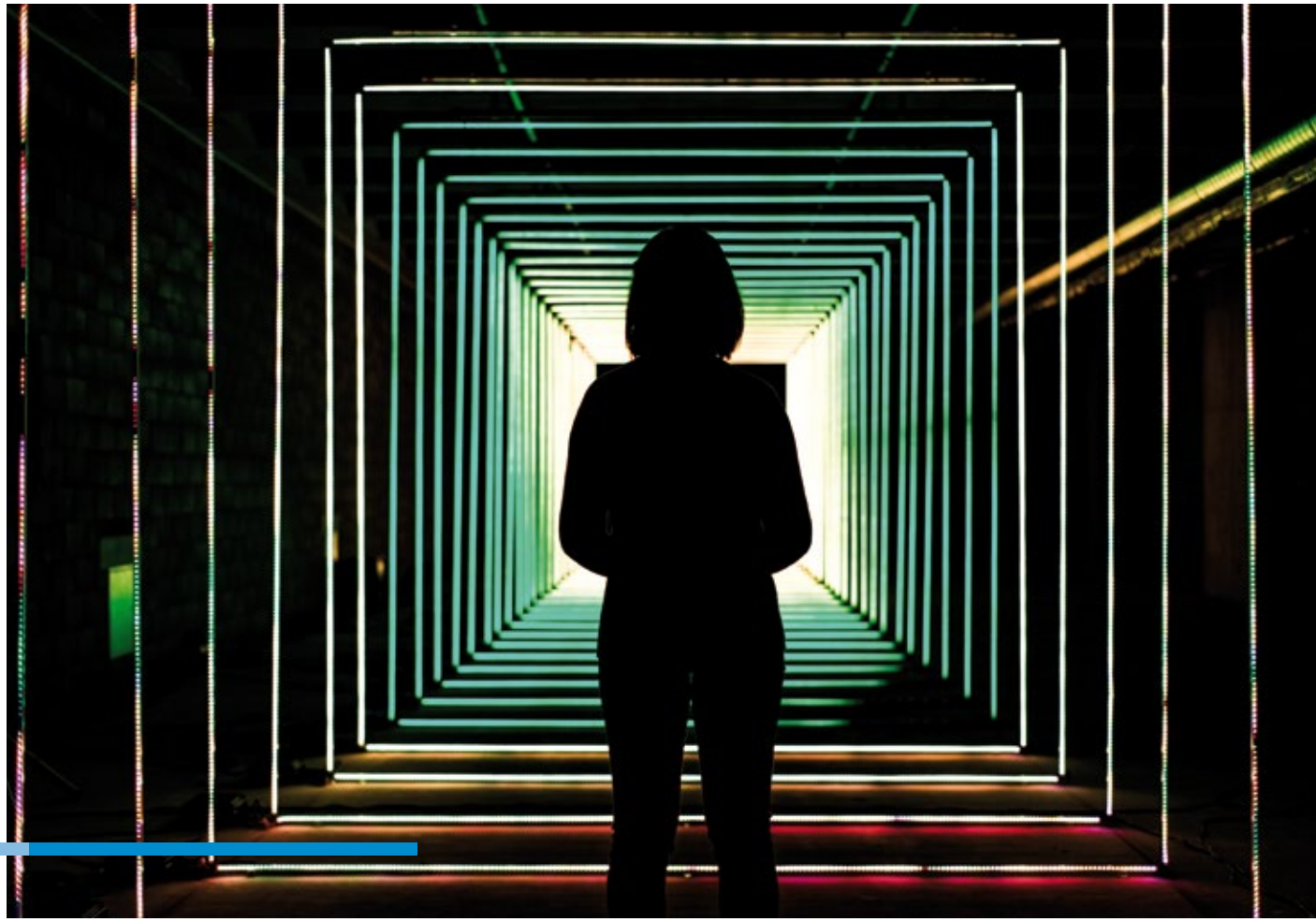


INFOGRAPHIC 3

Are online abuses, for example in the form of hate speech, harassment, hacking, privacy violations, or fraud, increasing?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019



Despite the agreement that online abuses (e.g., hate speech, harassment, hacking, privacy violations, or fraud) are increasing, the percentage of respondents that 'neither agreed nor disagreed' was substantial and many surveyed experts said the lack of empirical evidence made it difficult to answer this question.

This observation is both fair and important. It directs attention to the fact that there is currently a lack of reliable data, which, in turn, is linked to the need to standardize methods and initiatives to collect reliable data to inform policy decisions.

A recurring theme in comments made by surveyed experts is that while online abuses are increasing, so is the overall use of the internet – in other words, both abuse and normal use are increasing. One surveyed expert noted that this is a question of percentages versus absolute numbers. With more people online, and more layers of services and platforms, the absolute volume of both online abuse and the people affected by it increase. Yet this is a separate matter to whether there is an increase in the percentage of people misbehaving out of the overall body of internet users. Some surveyed experts also noted that as awareness of online abuses has increased, so too has the willingness to report abuses.

Both these factors may contribute to a perception that online abuses are increasing. A key trend here is that increasing awareness of, and sensitivity to, these abuses result in increasing political pressure to address them. This political pressure risks sparking uncoordinated, unilateral reactions that do not achieve desirable long-term effects.

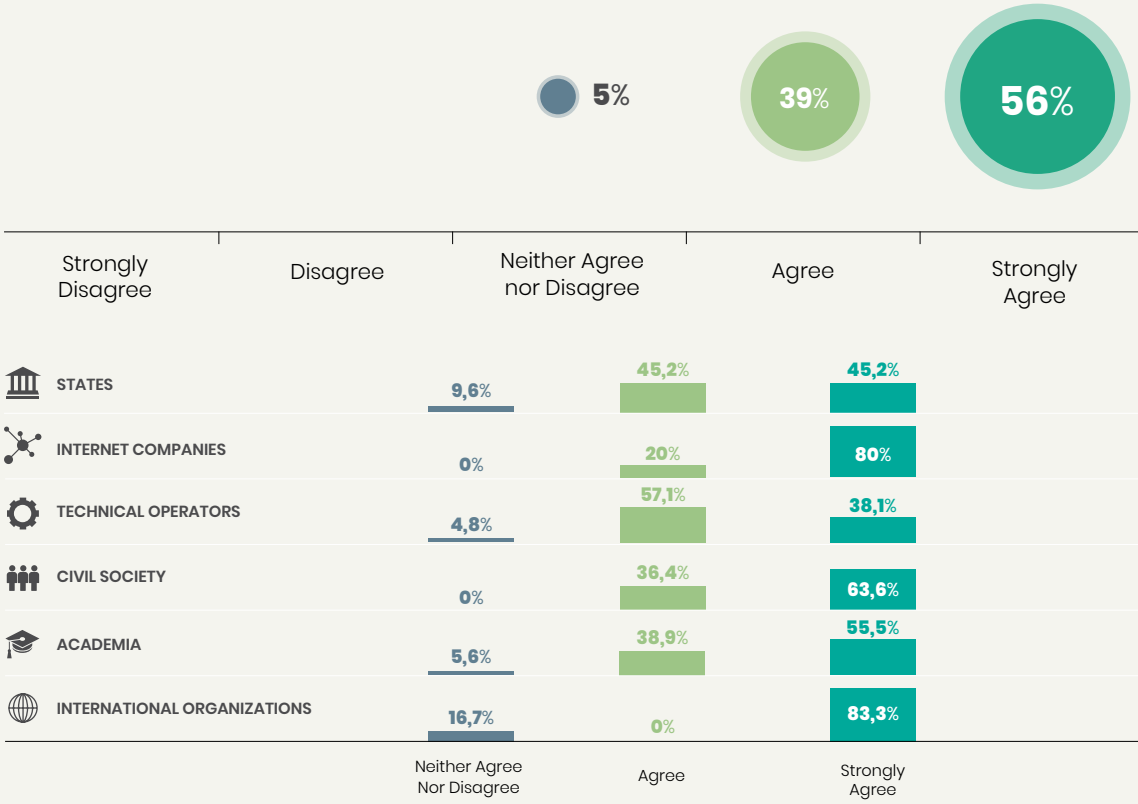
Some interviewed experts made the point that the internet merely mirrors conduct offline. One surveyed expert suggested that abuse is increasing both offline and online because of the current political and economic climate, and that online platforms simply reflect society. Different types of abuses emerge online, as well. The internet gives greater visibility to things that were heretofore largely restricted to the private sphere, and makes it easier for them to spread.

Another interviewed expert emphasized that these dynamics differ across cultures, and that there are increasing differences in what is seen as harassment, privacy violations and hate speech.

A majority (56%) of surveyed experts 'strongly agreed' that the cross-border legal challenges on the internet will become increasingly acute in the next three years. A further 39% 'agreed' and nobody 'disagreed' or 'strongly disagreed', while 5% responded that they have no view on this question.

INFOGRAPHIC 4

Will cross-border legal challenges on the internet become increasingly acute in the next three years?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

Comments provided by surveyed experts highlighted a widely held view that the combination of three factors will make cross-border legal challenges on the internet increasingly acute:

1. The world is increasingly becoming interconnected through the internet, thereby increasing diversity online;
2. The internet is deeply affecting societies and economies, meaning that the stakes are high; and
3. Nation states with different visions are seeking to increase their control over the internet, primarily by using national tools rather than transnational cooperation and coordination.

As one surveyed expert pointed out, in all this, the internet is neither the problem, nor the cause of the problem. Rather, the internet is the victim.

> "As one surveyed expert pointed out, in all this, the internet is neither the problem, nor the cause of the problem. Rather, the internet is the victim."

1.4

Competing legitimate interests need reconciling

A 'genuine regulatory challenge' exists where there are competing legitimate interests that are difficult to reconcile. In the context of internet jurisdiction, there are numerous instances of competing legitimate interests. For example, state A's protection of free speech may be difficult to reconcile with state B's restrictions on hate speech.

In more detail, the genuine regulatory challenges facing the ecosystem can be boiled down to the need to reconcile the three dimensions of:

1. fighting abuses;
2. protecting human rights; and
3. promoting the digital economy.

To a great extent, the difficulties in finding solutions to cross-border legal challenges on the internet stem from the fact that the genuine regulatory challenges are numerous and involve legal notions that are central to the very identity of each state. Yet this does not fully explain the complexity of the situation facing the ecosystem. Some of the challenges stem instead from the inadequacy of the legal concepts used.

1.5

Existing legal concepts are under stress

Most legal concepts with which we work – such as the focus on the location of evidence – were developed in the offline context.

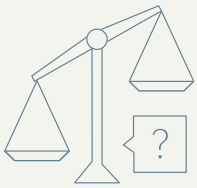
Their application online often involves decisions on the appropriate analogies and metaphors. The impact of such decisions was highlighted in the mid-1990s during the debate over the constitutionality of the US Communication Decency Act (CDA),[4] and was again on display in the 2016 Supreme Court of Canada hearing in the *Equustek* case.[5] Representing Google Inc, McDowell suggested that Google search was akin to a librarian that managed one of several card catalogues. In contrast, Justice Karakatsanis suggested a different analogy, comparing Google search to the person behind the counter of a bookstore. The choice of analogy would clearly impact the question of responsibility.

Several interviewed experts emphasized the concern that in the jurisdiction field, legal concepts are old fashioned and outdated. This creates 'artificial regulatory challenges' in that the frameworks and concepts being applied are insufficient to address the issues; in other words, the inadequacy of the tools may cause regulatory challenges. This prevents, or at least limits, progress.

Concerns about legal concepts

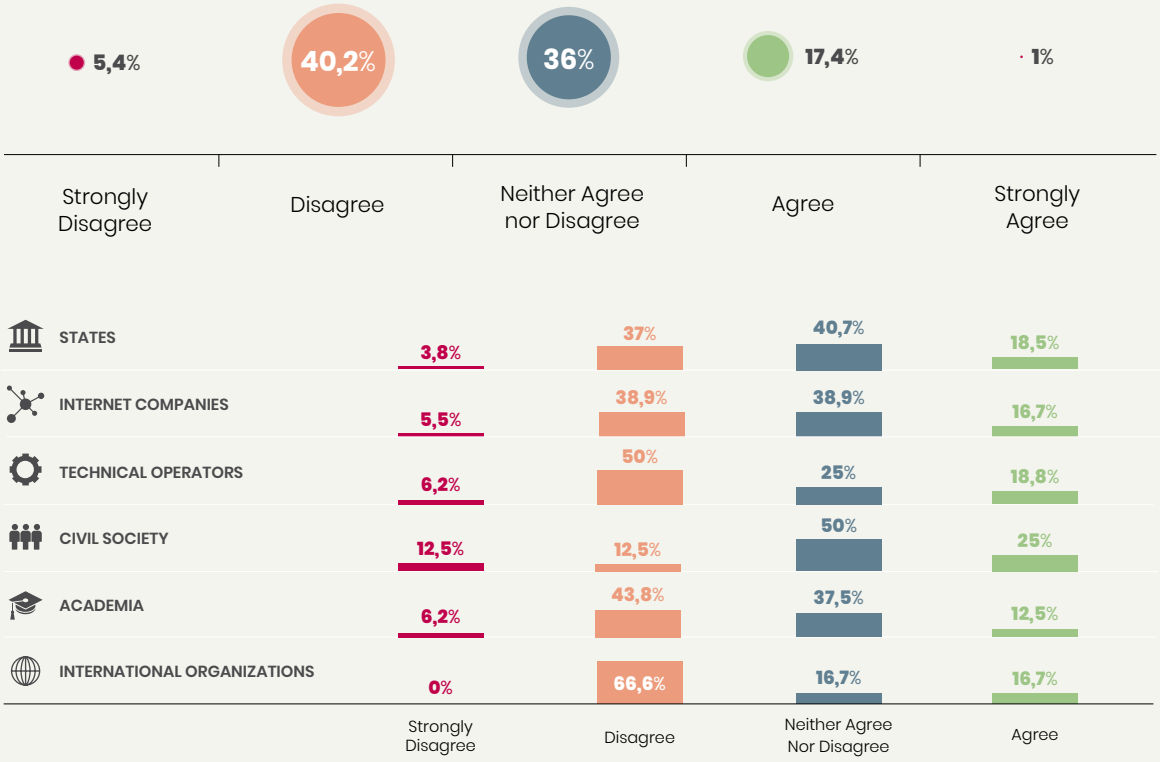
One of the survey questions posed the claim that we already apply the right legal concepts to address cross-border legal challenges on the internet. Among surveyed experts, 46% either disagreed or strongly disagreed, 36% indicated that they neither agreed nor disagreed, and 18% either agreed or strongly agreed.

4. Webach, K. (1997). Digital tornado: The internet and telecommunications policy. (Working paper of the Federal Communications Commission).
5. Google Inc v Equustek Solutions Inc 2017 SCC 34.



INFOGRAPHIC 5

Are we already applying the right legal concepts to address cross-border legal challenges on the Internet?



SOURCE; Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

Comments from surveyed experts offer guidance as to how these statistics should be understood, and what the concerns are. For example, one surveyed expert qualified their agreement with the above claim because although the basic legal concepts are sound and relevant, their application to the online environment remains a challenge. This concern is also recurring in the literature.

Another surveyed expert noted that there are several lacunae in the legal concepts, and yet another emphasized that there is a categorically new challenge in melding the global internet with national borders, and that we do not have the right legal concepts or principles for this task. The latter surveyed expert also made the point that this challenge is more complicated than other cross-border challenges, such as the regulation of financial transactions or airspace.

These survey responses correspond to observations commonly made in the literature. For example, the mobility of data undermines the utility of several traditional jurisdictional anchor points.

> "Too much of the discussion of cross-border legal challenges on the internet relies on legal concepts involving imprecise abstractions that are difficult to operationalize."

A related concern is that arguably too much of the discussion around cross-border legal challenges on the internet relies on legal concepts involving imprecise abstractions that are difficult to operationalize. In part, this is due to differing understandings of legal concepts. One example of this is found in the term 'comity,' which has a quite specific meaning in US law but remains a vague and controversial concept in international law. Due to the variations in legal systems around the world, one surveyed expert noted, it might be difficult to even assert which are the 'right legal concepts'. Another surveyed expert pointed out that while some regions of the world work with the 'right' legal concepts, we do not do so on a global level.

One surveyed expert noted that courts lack the right black letter law framework. However, the same expert also added that arriving at the right black letter law framework would not be so difficult and would not require any major reinvention of the law.

In this context, a potential barrier is the degree to which courts properly understand and keep up with technological developments. This challenge was once openly acknowledged by courts. Most famously, in 1997, the US District Court for the Southern District of New York observed that: "Judges and legislators faced with adapting existing legal standards to the novel environment of cyberspace struggle with terms and concepts that the average [...] five-year-old tosses about with breezy familiarity."[6] Today, one rarely sees such open admissions.

Due to the complexity involved, few areas are as plagued by artificial regulatory challenges as the debate about cross-border legal challenges on the internet. One need only consider the conceptual complexity involved in analyzing a standard cross-border legal issue, such as a claim of jurisdiction over conduct that occurs in another state but affects the state making the claim. In such a situation, tradition would dictate beginning with a consideration of whether the matter falls within public or private international law – a question that does not always have an obvious answer.[7]

If the matter falls under private international law, there is a need to consider other matters, such as whether there are grounds for claiming personal jurisdiction and subject matter jurisdiction. Then, there is a need to identify the applicable law and determine whether there are any grounds for the court in question to decline to exercise jurisdiction. Only then can the matter be heard. Once a judgment is issued, new issues arise around recognition and enforcement.

If the matter rather falls under public international law, tradition points to at least three different types of jurisdiction for consideration – prescriptive, adjudicative and enforcement jurisdiction, to which a fourth (investigative jurisdiction) has recently been added. Each of these types of jurisdiction is associated with unclear criteria, and it is not always obvious to which category a given matter would belong. For prescriptive jurisdiction, there is a set of commonly referenced principles known as the *Harvard Draft principles*[8], with the addition of the so-called 'effects doctrine'. These principles were originally drafted for a narrower purpose compared to how they are often treated today. The criteria are less clear for adjudicative and enforcement jurisdiction, however, and the detailed criteria for investigative jurisdiction remain to be developed.

If the claim of jurisdiction overcomes these hurdles, there are still numerous other considerations, such as:

- Would the claim of jurisdiction violate the sovereignty of another state?
- Would the claim of jurisdiction be contrary to the duty of non-intervention?
- Would the claim of jurisdiction be contrary to comity?
- Is the claim of jurisdiction in fact mandated by the due diligence principle?[10]

This conceptual complexity works as a 'barrier to entry', preventing the 'uninitiated' from contributing to the debate, and risks making this field the exclusive domain of a small group of specialist lawyers. It also regularly results in misunderstandings and miscommunication. Furthermore, it creates an environment in which discussions are characterized by overly broad and simplistic claims, leading to locked positions; too often, the legal concepts are not debated in a systematic manner. Instead, there is a tendency to pick and choose concepts that support any given position.

A proponent of a claim of jurisdiction may, for example, feel vindicated by the 'effects doctrine' (while ignoring all other principles), while an opponent to the same claim may feel vindicated by the 'comity principle' (while ignoring all other principles). The complexity may hide the flaws in their respective approaches, and because they both feel supported by law, the likelihood of agreement – or even of a constructive discussion – is low. This highlights a clear need for

---

6. American Libraries Association v Pataki 1997 SDNY 969 F Supp 160, 170 (per Preska J).

7. Or 'conflict of laws' as 'private international law' often is referred to in Common Law countries.

8. Introductory Comment to the Harvard Draft Convention on Jurisdiction with Respect to Crime 1935. (1935). Supplement *American Journal of International Law*, 29, 443, p. 445.

9. See Chapter 5 'Relevant concept clusters 101' for definitions of these concepts.

a simpler legal framework of foundational principles in which to anchor the discussion. The Report points to a possible overarching jurisprudential framework for jurisdiction in which attention is directed at three criteria:

1. whether there is a substantial connection between the matter and the state seeking to exercise jurisdiction;
2. whether the state seeking to exercise jurisdiction has a legitimate interest in the matter; and
3. whether the exercise of jurisdiction is reasonable given the balance between the state's legitimate interests and other interests.

These criteria transcend the perceived gap between public and private law, and can incorporate both effects doctrine and comity, as well as other relevant public and private international law concepts. As such, they amount to a suitable foundation upon which to build more detailed legal norms for specific contexts.

Current discussions of cross-border legal challenges on the internet predominantly focus on tackling the most pressing day-to-day issues (i.e., some of the genuine regulatory challenges), at the expense of focusing on the underlying conceptual complexity (i.e., the artificial regulatory challenges). This is natural, given the impact that these challenges have for society. However, real progress can only be made if the ecosystem also tackles the artificial regulatory challenges. Indeed, the artificial regulatory challenges must first be addressed in order to adequately address the genuine regulatory challenges. It is hoped that this Report can contribute to this important task.

To this end, the subsequent Chapters of this Report take care to not only engage with and outline the genuine regulatory challenges, but to do so in a manner that may mitigate some of the artificial regulatory challenges alluded to here.

"Current discussions of cross-border legal challenges on the internet predominantly focus on tackling the most pressing day-to-day issues (i.e., some of the genuine regulatory challenges), at the expense of focusing on the underlying conceptual complexity (i.e., the artificial regulatory challenges)."

1.6

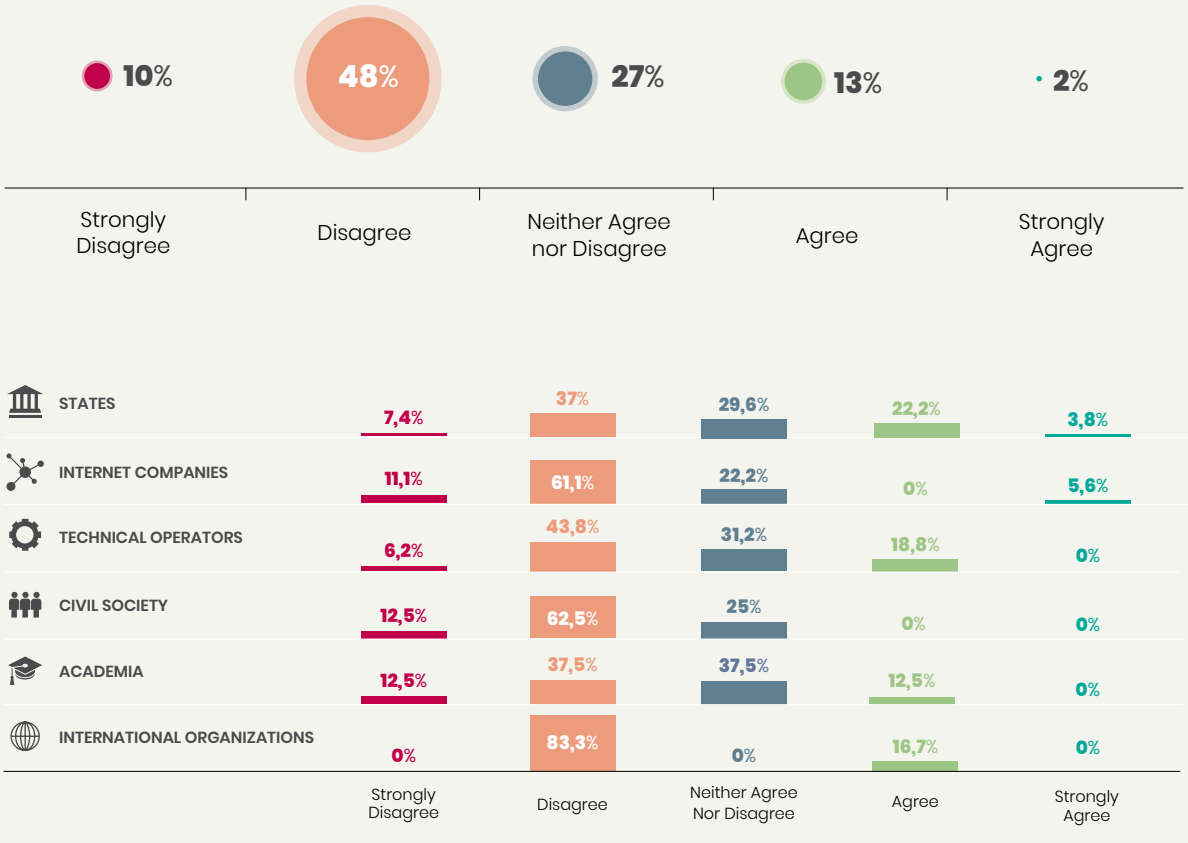
Proper frameworks and institutions are lacking

The Internet & Jurisdiction Policy Network's stakeholders pointed to a current lack of appropriate institutions to address cross-border legal challenges on the internet.

The majority (58%) of surveyed experts either 'disagreed' or 'strongly disagreed' that we already have the right institutions in place to address cross-border legal challenges on the internet. Only 15% of surveyed experts stated either 'agreed' or 'strongly agreed', while 27% indicated that they neither 'agreed' nor 'disagreed'.

INFOGRAPHIC 6

Do we have the right institutions to address cross-border legal challenges on the internet?



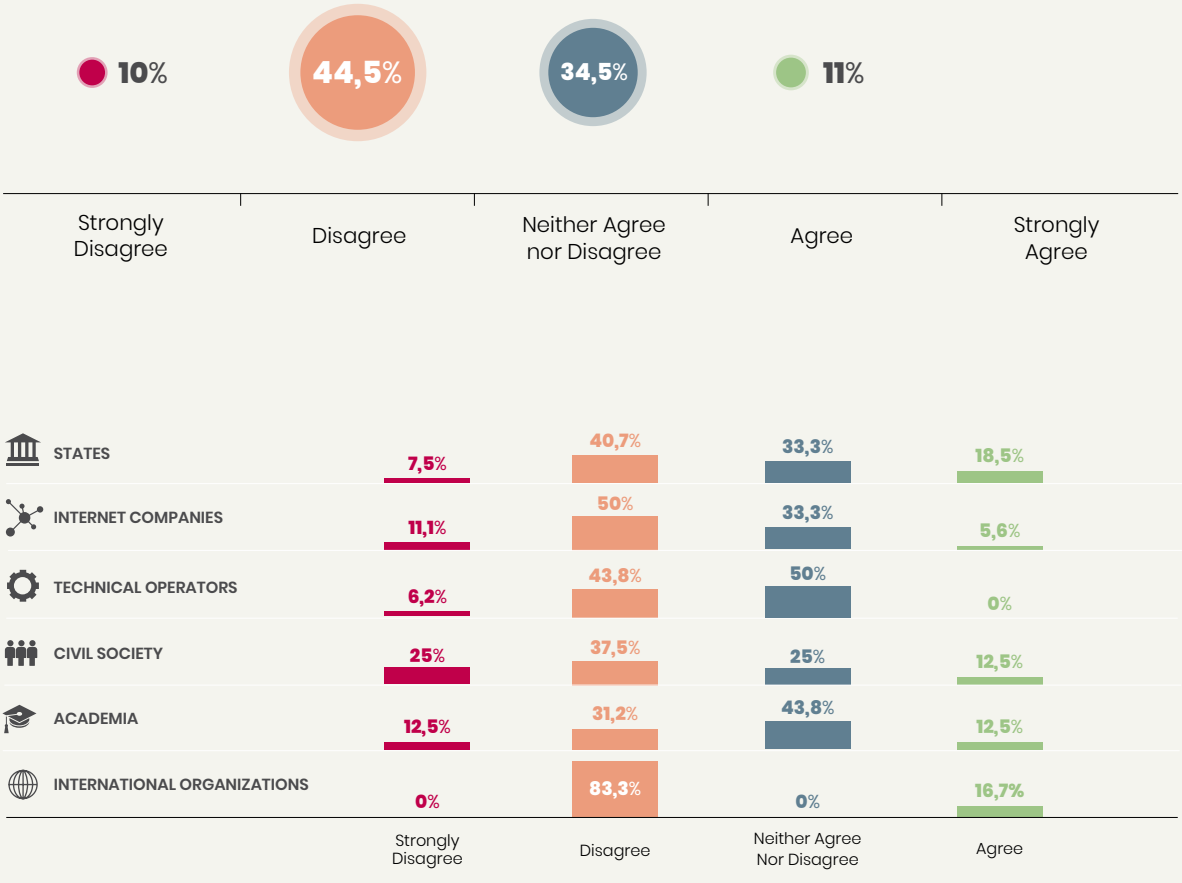
SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

Some surveyed experts commented that awareness of the sensitivity of cross-border legal challenges on the internet is often low in current institutions – both internationally and domestically – and that they need to evolve and better cooperate with one another. Among surveyed and interviewed experts, there was a clear majority view that although numerous institutions work on these issues, additional fora or institutions might be beneficial. A smaller number expressed doubt about the need for additional institutions.

Another aspect of lacking coordination relates to the availability of appropriate frameworks and standards. 44.5% of surveyed experts 'disagreed', and a further 10% 'strongly disagreed', with the assertion that we have the frameworks and standards to address cross-border legal challenges on the internet. Only 11% of surveyed experts 'agreed', and none 'strongly agreed'. 34.5% of surveyed experts indicated that they neither 'agreed' nor 'disagreed'.

INFOGRAPHIC 7

Do we have the right frameworks and standards to address cross-border legal challenges on the internet?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

In their comments, surveyed experts pointed to regional differences, with some noting that global standards do not exist and are unachievable. Others pointed out that the cross-border legal challenges on the internet are being addressed under ordinary domestic laws, with some adding that many cross-border challenges cannot effectively be addressed within the national domain. This highlights several things:

1. states are attempting to address these issues by applying their existing laws;
2. but national responses are inadequate; therefore,
3. there is a clear need for transnational coordination and cooperation.

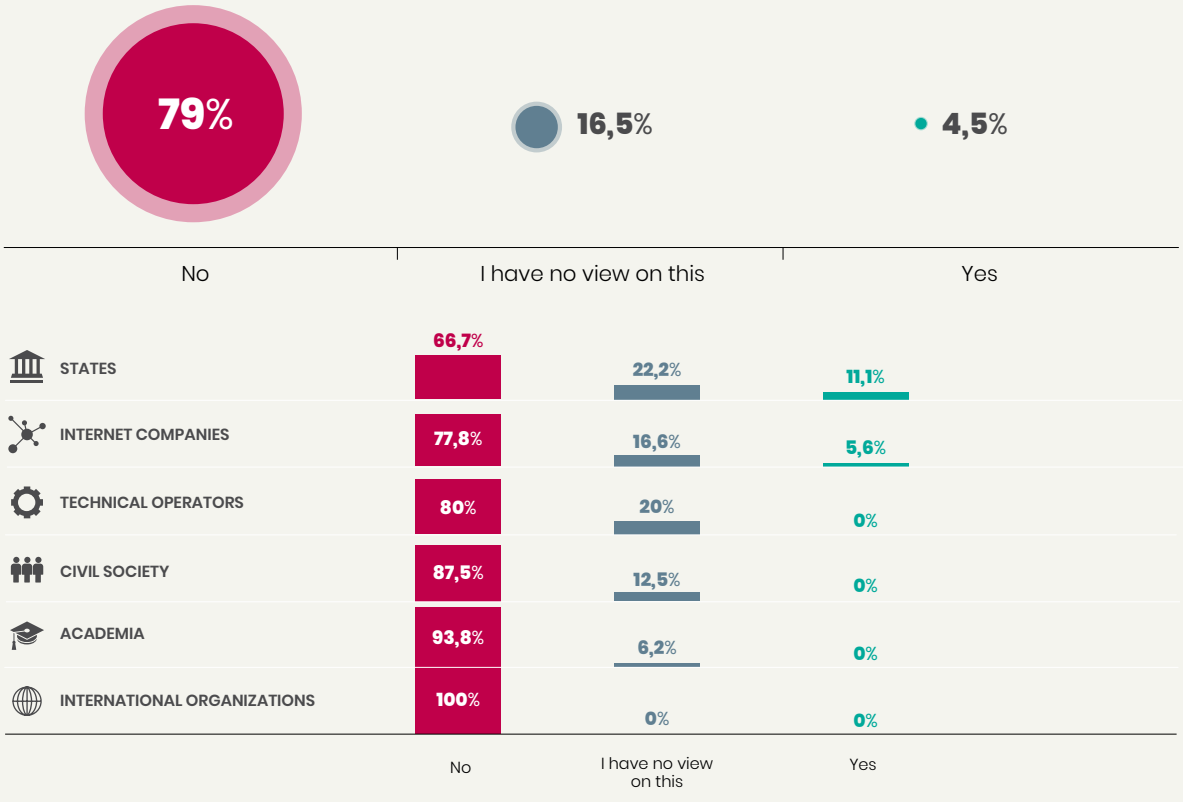
1.7
Coordination is insufficient

The stakeholders sent a strong message that current coordination efforts are insufficient.

Asked whether there is sufficient international coordination and coherence to address cross-border legal challenges on the internet, no less than 79% of surveyed experts answered 'no', while only 4.5% answered 'yes'. 16.5% responded that they have no view on this question.

INFOGRAPHIC 8

Is there sufficient international coordination and coherence to address cross-border legal challenges on the Internet?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

While the survey result shows a clear and overwhelming consensus across stakeholder groups and regions, it should be noted that some surveyed experts said robust international coordination and cooperation can be seen among certain groups and in certain sectors. One example mentioned was coordination among law enforcement agencies, e.g., via the work of Interpol, Europol and the Council of Europe.

1.8

Fundamental attributes of the internet are at stake

Should the internet be preserved? While the vagueness of this question is obvious, the instinctive answer is probably still a resounding 'yes'. After all, the internet has already revolutionized how people, businesses and governments interact; it plays a central role in the lives of billions of people, and has brought numerous significant economical and societal benefits.

At the same time, it is widely recognized that the internet is constantly evolving. This is perhaps particularly true in developing countries, where the internet's uptake, structure and usage are evolving quickly. As the way we use the internet has changed over the years, so too has the content available online and the internet's technical infrastructure. Online, change is constant and natural, and it typically translates into desirable progress.

Nevertheless, there are perhaps certain characteristics of the internet that ought to be shielded against change. If so, what might those characteristics be? What is it about the internet that instinctively deserves to be preserved? These kinds of questions may be answered at different levels of abstraction. At a relatively high level, one might point to the internet's openness, and its role as an enabler and protector of human rights and democratic values, as qualities that are particularly worth preserving. Other such qualities include the internet's potential to contribute to a fairer and more equitable world, and to bring people closer together through a global communications medium, ultimately supporting a peaceful coexistence.

Unfortunately, all these characteristics are currently under threat, to varying degrees, and they cannot be taken for granted. Rather, it must be recognized that the internet is a fragile environment and that the characteristics of the internet that are to be preserved must be actively protected. Two such characteristics are the internet's cross-border and permission-less nature – both of which are under threat.

> "The characteristics of the internet that are to be preserved must be actively protected."

1.8.1

The cross-border internet cannot be taken for granted

As noted in a brief September 2018 Internet Society concept note on the internet and extra-territorial effects of laws: "Globalization is a feature of the internet, not a bug, and legal systems everywhere should recognize this, not try to 'fix' it."[10] This observation is both accurate and important. Yet as discussed in detail below, the regulatory landscape online (and offline) has always been fragmented. This is a direct consequence of the sovereignty that states enjoy, insofar as they have the capacity to make their own laws. Indeed, it has been noted that the difficulty of applying and enforcing any regulatory system online may be attributed to the fact that the internet's operation involves a highly fragmented universe of actors, norms, procedures, processes and institutions, including many non-state entities.[11]

Although this kind of fragmentation is nothing new in the online ecosystem,

10. Internet Society. (2018, September). *The internet and extra-territorial application of laws*. Retrieved from https://www.internetsociety.org/wp-content/uploads/2018/10/The-internet-and-extra-territorial-application-of-laws-EN.pdf, p. 1.

11. Kuner, C.. (2017, February 1). The internet and the global reach of EU Law. *Law Society Economy Working Papers* No. 4/2017. Retrieved from SSRN: https://ssrn.com/abstract=2890930 or http://dx.doi.org/10.2139/ssrn.2890930, p. 7.

states are making increasingly aggressive jurisdictional claims and backing up those claims with heavy fines or even the threat of imprisonment, raising the stakes for the subjects of regulations. Therefore, both natural and legal persons may opt to avoid being present on certain markets. For example, those wishing to avoid contact with certain states may utilize technical measures such as the geo-location technologies, or non-technical measures such as disclaimers or terms of service.

Whether technical or non-technical, this type of fragmentation – if widespread – is a threat to the cross-border internet, and carries both societal and economic consequences. Fragmentation online contributes to fragmentation offline, resulting in a loss of some useful interactions and cross-border engagements that may spark mutual trust and understanding. As to the financial side, it has been noted that: "The balkanization of the internet will change how companies do business. This will likely reduce efficiency and, in a macro way, have some effect on the global economy."[12]

At the same time, it may be argued that some degree of fragmentation is the only way to uphold national rules – which may be necessary to avoid a lawless internet – and avoid claims of global scope of jurisdiction. The task, then, is to determine the type and degree of acceptable fragmentation, without endangering the characteristics of the internet that should be shielded from change.

In a sense, what we are witnessing is a decreasing gap between the initially borderless internet and the territorially grounded legal systems; the internet is becoming less 'borderless', and legal systems are becoming less anchored in territoriality. If properly coordinated and managed, this development stands to provide great benefits to both the fight against abuses and the protection of human rights, as well as the digital economy. If mismanaged, however, it may spell disaster for the online environment.

Yet fragmentation also occurs in a more technical sense. A useful distinction has been made between fragmentation *on* the internet, as discussed above, and fragmentation *of* the internet – fragmentation of the internet's underlying physical and logical infrastructures.[13]

The physical backbone of fiber optic cables crossing oceans and international borders enables a relatively seamless online experience regardless of location. Traditionally, these cables have been controlled by telecommunications operators, but a shift in own-

---

12. PwC. (2018). *Revitalizing privacy and trust in a data-driven world.* Retrieved from https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf

13. World Economic Forum. (2016). *Internet fragmentation: An overview.* Retrieved from http://www3.weforum.org/docs/WEF_FII_internet_Fragmentation_An_Overview_2016.pdf, p. 3.

ership has given rise to at least two 'new' types of owners. The first is the major internet companies. Some of these companies have invested in their own trans-oceanic cables, resulting in private networks that connect their data centers and operate outside of the rules that have governed the internet and its network operators to date, such as those pertaining to common carriage and neutrality.[14]

The second category of new cable owners includes nation states seeking to pursue geo-political cyber strategies. China, most notably, is making significant investments to build a geographically strategic infrastructure that allows data to flow around the world entirely on Chinese-owned fiber optic infrastructure.[15] Such a nation-controlled infrastructure may be applied in order to reduce access to information, limit participation in online forums, restrict data privacy and freedom of expression, and perhaps embed surveillance and censorship capabilities.[16] These developments could be seen as a logical extension of the Great Firewall of China, and may in fact make the current Great Firewall of China redundant. At any rate, they represent a serious attack on the neutrality of the internet's core infrastructure. Furthermore, they represent a step away from the internet as a 'network of networks' – a key feature that encourages a multistakeholder approach to internet governance – and pose a threat to the cross-border internet.

Another technological step that may lead to fragmentation is the Russian government's ambitions to develop a separate backup of system of Domain Name Servers (DNS), which, according to 2017 reports, would not be subject to control by international organizations.[18] The Press Secretary of the Russian Presidency has specified that Russia does not intend to disconnect from the global internet, arguing instead that recent unpredictability from the US and EU demanded that Russia be prepared for any turn of events.[18] On February 11, 2019, it was reported that Russia has taken several major steps in this direction.[19]

Furthermore, major satellite-based internet connectivity, while largely in its infancy, may have the potential to facilitate and accelerate fragmentation of the internet.

In a sense, the fragmentation of technical infrastructure likely poses a greater threat to the global internet than fragmentation arising from the regulatory landscape online. Moreover, while there is a degree of political will to attempt to overcome the negative effects of fragmentation sparked by regulatory challenges, there are currently no signs of any developments that may prevent or even slow down the fragmentation of technical infrastructure.

In tackling these issues, it is essential to keep in mind that the cross-border internet cannot be taken for granted; it is a resource that needs to be actively protected. Indeed, the cross-border internet – both from a technical and regulatory perspective – is a sensitive and fragile environment comprising multiple stakeholders and actors; changes for one stakeholder group may have irreversible flow-on consequences for others.

1.8.2

The permission-less nature of the internet needs active protection

A distinctive feature of the online environment is its permission-less nature. In setting up a website, for example, one may be responsible and liable for that website, but no permission is required to launch it. By removing barriers to entry, the permission-less nature of the online environment has been a great facilitator of innovation, and its importance is widely recognized. One of the NETmundial principles articulates this importance:

"The ability to innovate and create has been at the heart of the remarkable growth of the internet and it has brought great value to the global society. For the preservation of its dynamism, internet governance must continue to allow permission-less innovation through an enabling internet environment, consistent with other principles in this document. Enterprise and investment in infrastructure are essential components of an enabling environment."[20]

The EU's e-commerce Directive from 2000 includes another articulation of

---

14. Song, S. Internet drift: How the internet is likely to splinter and fracture. *Digital Freedom Fund*. Retrieved from https://digitalfreedomfund.org/internet-drift-how-the-internet-is-likely-to-splinter-and-fracture/.

15. Song, S. Internet drift: How the internet is likely to splinter and fracture. *Digital Freedom Fund*. Retrieved from https://digitalfreedomfund.org/internet-drift-how-the-internet-is-likely-to-splinter-and-fracture/.

16. Song, S. Internet drift: How the internet is likely to splinter and fracture. *Digital Freedom Fund*. Retrieved from https://digitalfreedomfund.org/internet-drift-how-the-internet-is-likely-to-splinter-and-fracture/.

17. Internet & Jurisdiction Policy Network. (2017, December). Russia reportedly moves ahead with plan to create independent DNS backup for BRICS countries. I&J Retrospect Database. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-6626_2017-12.

18. RT. (2018, February 20). *Russia to launch 'independent internet' for BRICS nations - report*. Retrieved from https://www.rt.com/politics/411156-russia-to-launch-independent-internet/.

19. Cimpanu, C. (2019, February 11). Russia to disconnect from the internet as part of a planned test. *ZD Net*. Retrieved from https://www.zdnet.com/article/russia-to-disconnect-from-the-internet-as-part-of-a-planned-test/.

20. NETmundial Initiative. The *NETMundial Principles*. Retrieved from http://netmundial.org/princi

the permission-less nature of the online environment. Article 4(1) emphasizes that: "Member States shall ensure that the taking up and pursuit of the activity of an information society service provider may not be made subject to prior authorisation or any other requirement having equivalent effect."[21] The fact that the internet, by tradition, has been a network of networks without a central authority has assisted – or even necessitated – the permission-less nature discussed here. However, with the move toward infrastructure-level fragmentation, the permission-less nature cannot be taken for granted in the future. Rather, it must be actively protected and preserved.

1.9

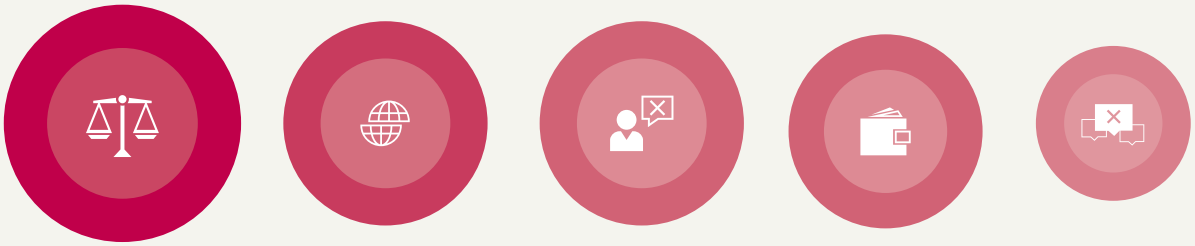
Not addressing jurisdictional challenges comes at a high cost

A failure to properly address the cross-border legal challenges on the internet will result in high costs for all stakeholders and may cause irreparable harm. Such negative consequences were highlighted in surveys and interviews.

When asked what, if any, negative consequences they foresee if cross-border legal challenges on the internet are not properly addressed, the Internet & Jurisdiction Policy Network's stakeholders highlighted the following:

INFOGRAPHIC 9

What negative consequences, if any, do you foresee if cross-border legal challenges on the Internet are not properly addressed?



60% Legal Uncertainty

54% Loss of some key cross-border benefits of the Internet

54% Restrictions of expression

52% Compliance costs for online businesses

35% Inability to address online abuses

Top 5 answers by respondents

SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

In their comments, surveyed experts also identified the lack of rules to govern conduct on the internet as a risk. As one surveyed expert noted, as in every game with no rules, it is the strongest that will prevail.

---

21. *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, Article 4(1).

1.10

A multistakeholder approach is still desired

The idea that internet governance requires joint management of internet resources by governments, business and civil society in their respective roles – i.e., multistakeholderism[22] – remains the preferred approach to addressing cross-border challenges on the internet[23]. This was a clear theme among surveyed and interviewed experts.

Many interviewed experts pointed to multistakeholder models currently operating in certain spaces, such as governments working with social media companies in a collaborative or cooperative approach to combat issues like child abuse material or extremist activity online. Some specific examples cited include the activities of Internet Corporation for Assigned Names and Numbers (ICANN) and the associated Regional At-Large Organizations,[24] the World Wide Web Consortium (W3C)[25] and the Internet Governance Forum (IGF), including its regional initiatives.[26] However, interviewed experts considered that there must be more robust interaction across more areas. For example, one interviewed expert said civil society and citizens must have a stronger voice in these discussions. Another interviewed expert stressed the importance of a multistakeholder model that incorporates industry agreement, as opposed to absolute oversight by government – an agile and flexible system that can allow issues to be addressed as they arise.

Another expert commented that we are seeing threats or attempts to undermine the multistakeholder approach, particularly due to unilateral initiatives from governments and private sector actors driven by their own national or commercial interests.

Thus, the message was clear that while a multistakeholder approach is still desired, the multistakeholder model is yet to be perfected.

> "The message was clear that while a multistakeholder approach is still desired, the multistakeholder model is yet to be perfected."

Additionally, some interviewed experts pointed to an important gap in the widespread reliance on multistakeholderism. Court decisions have a significant impact across all cross-border legal issues on the internet. Yet by their nature, court decisions are not reached through any process that may be described as multistakeholderism. Typically, only parties to the dispute are in a position to present arguments to courts. There is therefore an obvious risk that important interests are unrepresented at trials and overlooked by courts.

To address this weakness in the judicial system, some courts allow the filing of so-called *amicus curiae* – 'friend of the court' – briefs. Courts have allowed a large number of *amicus* briefs in some recent high-profile internet jurisdiction cases, such as the *Micro-*

---

22. See e.g.: UNESCO. (2017). *What if we all governed the internet? Advancing multistakeholder participation in internet governance.* Retrieved from https://en.unesco.org/sites/default/files/what_if_we_all_governed_internet_en.pdf.

23. For a 2019 example, see: GSMA. *Digital Declaration*. Retrieved from https://www.gsma.com/betterfuture/digitaldeclaration.

24. *For example, the African Regional At-Large Organization, the Asian, Australasian and Pacific Islands Regional At-Large Organization, the European Regional At-Large Organization, the Latin American and Caribbean Islands Regional At-Large Organization and the North American Regional At-Large Organization.*

25. World Wide Web Consortium. Retrieved from http://www.w3.org/Consortium/.

26. *For example, the Latin America and Caribbean IGF, East Africa IGF, Central Africa IGF, North Africa IGF, West Africa IGF, Central Asia IGF, Asia Pacific IGF and Arab IGF.*

soft Warrant case[27] heard in the US Supreme Court in February 2018.

Such accommodation of *amicus* briefs is an exception, however, and most courts avoid non-party input by: (1) not allowing *amicus* briefs at all, (2) adopting court rules that exclude *amicus* briefs in all but the most exceptional circumstances, or (3) interpreting the court rules restrictively to exclude non-party input. Restrictive approaches toward *amicus* briefs may be justified by the risk of delays and added costs. These are legitimate concerns, and courts are typically restrictive when it comes to *amicus* briefs filed by foreigners, in particular. At the same time, though, the stakes are often high for non-parties, as well, including foreign non-parties.[28] In cases where courts feel empowered to make decisions with international impact, one may argue that they should accept the responsibility of ensuring that they are sufficiently exposed to the international interests that stand to be impacted by their decisions.

In light of the above, reform of the *amicus curiae* system is arguably the most urgently needed enhancement of multistakeholderism.

1.11

A pressing challenge, insufficiently addressed

The cross-border legal challenges facing the internet are currently getting more attention in media and in policy discussions than ever before.

In many ways, the challenges faced in the context of internet jurisdiction are akin to the challenges the world is facing in the context of climate change. Both challenges can only be addressed through cross-border cooperation and coordination, and both have a global impact that affects developing countries most acutely. Both challenges are also of a nature that might make individuals (and even individual states) feel unable to do anything of impact on their own to affect change.

Furthermore, one may argue that the online environment is now facing its own form of climate change. Like the 'tipping points' that scientists have pointed to in the context of climate change, this Report highlights that if developments continue along the current course, we will sooner or later reach similar tipping points at which the internet as we know it ceases to exist – and from which attempts at a reversal are potentially futile. But there are also important differences between the respective crises unfolding in the natural environment and the online environment. For example, while short-term economic arguments are often levied against proposals for decisive action against climate change, there are few if any economic arguments against tackling the cross-border legal challenges on the internet. On the contrary, decisive action against the cross-border legal challenges on the internet will also be rewarded economically in the short-term, not just in the long-term.

Furthermore, while there are still climate change deniers, few doubt or even question the very real negative impact of not addressing the cross-border legal challenges on the internet. More broadly, while it has been suggested that some states prefer to operate with an unclear and chaotic legal framework regarding matters such as cyber espionage and cyber aggression, there are few that benefit from jurisdictional chaos and 'hyperregulation' online. These latter points suggest that there ought to be a clear political will, and unquestioned economic and social justifications, to decisively tackle the challenges faced in the context of internet jurisdiction.

---

27. Wikipedia. Microsoft Corp. v United States. Retrieved from https://en.wikipedia.org/wiki/Microsoft_Corp._v._United_States.

28. Consider e.g., the Supreme Court of Canada's approach to *amicus* briefs in *Google Inc. v. Equustek Solutions Inc.*. Retrieved from https://www.scc-csc.ca/case-dossier/info/dock-regi-eng.aspx?cas=36602.

02

OVERARCHING TRENDS

—

EXPRESSION

SECURITY

ECONOMY

The combination of detailed desk research and stakeholder input – via the survey and interviews – drew attention to several overarching trends that are central to any discussion of the cross-border legal challenges on the internet. These overarching 'meta-trends' are shaping topical trends, and to a degree, they are setting the parameters within which the legal and technical approaches may be explored.

First, some of the overarching trends relate to the changing technological landscape, which creates a need for 'future-proofing' any legal or technical approaches we embark on today. In this context, there is a clear trend of eroding borders between the online, data-driven world and the physical world, and there is an equally clear trend of continuing migration to the cloud.

Second, some of the overarching meta-trends relate to the regulatory environment on the internet. While perhaps a rudimentary observation, there is a clear trend of recognition that legal regulation is necessary online – the question of whether to regulate or not is a 'dead issue'. A proliferation of initiatives signals that the cross-border legal challenges on the internet are being taken seriously, perhaps more so than ever before. Yet the measures taken suffer from a lack of coordination and cooperation. This only compounds challenges arising from the trends of information overload and information access problems.

A third trend concerns serious attempts at re-thinking the role of territoriality for the regulation of the internet, and an emerging political will to do so. Indeed, there is increasing recognition, in some settings, that territoriality is largely irrelevant. Lawmakers are also displaying a greater appetite for extending laws online, often in an 'extraterritorial' manner that affects individuals, businesses and organizations overseas, or indeed other states; we may now be in an era of jurisdictional 'hyperregulation'. The increasing geographic reach of national laws may be seen as a natural response when national laws are the only tools to address transnational issues. Nevertheless, this trend is associated with several severe issues, including enforcement difficulties, and there is some irony in that applying more laws transnationally will encourage more cooperation, because it is necessary for enforcement.

Fourth, there is a set of overarching trends that relate to normative plurality, convergence and cross-fertilization. Blurring the distinction between illegal content, content that violates terms of service and content that is objectionable has only augmented the diversity of normative sources. One trend observed in this context is a harmonization via company norms; another is judicial cross-fertilization driven by replication and imitation that does not always properly account for scalability issues. In this context, the Internet & Jurisdiction Policy Network's stakeholders pointed to a trend of newer and smaller actors being bound by decisions from established and larger actors.

A fifth trend pertains to the increased complexity around the role of internet intermediaries. In some instances, these intermediaries are self-proclaimed gatekeepers; in others, they are involuntary gatekeepers. Sometimes, they are simply scapegoats and 'easy' targets for litigation and content restriction orders.

2.1

A technological landscape in constant flux

There is a necessary and constant interplay between law and technology, as developments in one sphere are likely to impact the other.

This is true both online and offline. In the past, such developments were typically slow, gradual and relatively sporadic. In the online environment, however, major technological developments are fast, dramatic and numerous. This puts significant stress on the law-making apparatus and demands a degree of future-proofing that goes far beyond what has historically been required. The preparedness for this task often appears limited in industrialized countries and is nearly absent in many developing countries.

2.1.1

The unification of online and physical worlds

One clear overarching trend is the fact that borders between the online, data-driven world and the physical world are eroding and becoming less clear, or even meaningless. This is an ongoing process and not something new. People no longer 'go online' – they are constantly online. This has been the case for several years, in large part due to the uptake of smartphones.

In the Internet of Things era, however, the speed with which these borders erode is increasing dramatically, with effects for all aspects of society. As one interviewed expert noted, the big data-driven companies we know from the online environment are increasingly using their data-focused expertise to expand into traditional industries in the physical world (self-driving cars are one example, but this trend extends far beyond that). By the same token, traditionally offline companies are increasingly repositioning themselves as data-driven companies, but may still lack the capacity to fully engage with the breadth of cross-border jurisdictional issues because they are 'late to the party'. This raises several legal issues around competition, for example, and the abuse of dominant market positions, and we may have not yet seen the full picture of how it will impact cross-border legal challenges on the internet.

As several interviewed experts pointed out, technology in this context acts not only as an object of regulation, but as a regulatory force itself. Indeed, it has long been recognized that technology competes with law as a regulatory force.[29]

2.1.2

A continuing migration to the cloud

Put simply, cloud computing involves the on-demand provision of computing resources over the internet.[30] In this area, a distinction is routinely drawn between infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). All these forms of cloud computing have profound implications for cross-border legal challenges on the internet.

Whether intentionally or not, cloud computing typically creates connecting points to foreign jurisdictions in situations that may have previously been entirely domestic. Furthermore, cloud computing results in data being held by parties other than those who actually 'own' the data, which has consequences in relation to data privacy law, for example, and the ability of law enforcement to access content needed as evidence.

Cloud computing, with its often highly fluid data flows, may make it difficult or even impossible[31] to ascertain, in real time, where specific data is located. This, in turn, severely undermines the usefulness of data location as a jurisdictional connecting factor or focal point. As argued recently by a US court,

---

29. Lessig, L. (1999). The law of the horse: What cyberlaw might teach. *Harvard Law Review*, 113, 506.

30. See further: Millard, C. (Ed.). (2013). *Cloud Computing Law*. Oxford, United Kingdom: Oxford University Press

31. In re Search Warrants Nos 16-960-M-01 and 16-1061-M to Google, para 7.

when it is impossible to ascertain the location of data, it also becomes harder to argue that the sovereignty of a particular state was implicated when that data was accessed by a law enforcement agency: "Even if the interference with a foreign state's sovereignty is implicated, the fluid nature of Google's cloud technology makes it uncertain which foreign country's sovereignty would be implicated when Google accesses the content of communications in order to produce it in response to legal process."[32]

It is important, of course, to not confuse the question of *which* state's sovereignty is being interfered with, and the question of whether *any* state's sovereignty is being interfered with. The court's reasoning here may be accused of failing to recognize this distinction. Nevertheless, there is certainly some merit in the issue to which the court seeks to bring our attention.

While the study of cloud computing as a distinct regulatory or legal field seems to have declined, technological development is ongoing. Furthermore, states,[33] businesses,[34] and regions[35] are still developing ways in which they use cloud computing, and not all attempts at establishing cloud computing arrangements have been successful. One interviewed expert stressed that it is not only data that goes into the cloud. As massive amounts of software move into the cloud environment, ensuring control and security is a challenge, and security is not always built in from the start. Consequently, there is little doubt that cloud computing will continue to impact cross-border legal challenges on the internet as an overarching meta-trend.

2.2

Regulation: not if, but how

It is useful to distinguish between regulation *of* the internet, on the one hand, and regulation *on* the internet, on the other. The latter is now primarily in focus.

2.2.1

To regulate or not is not the issue

During the 1990s, a debate raged about whether it was possible to regulate Cyberspace, and whether it was even desirable to do so. This debate took place on several levels; in policy circles and in academia, and domestically and internationally among the comparatively limited number of states that were active online at that time. In the academic arena, key contributions to the English-language debate were made by several prominent North American scholars.[36]

Most famously, in the policy context, 1996 saw Barlow present his well-known *Declaration of the Independence of Cyberspace*, which captured the spirit of the time:

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. [...] You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. [...] Cyberspace does not lie within your borders. [...] Ours is a world that is both everywhere and nowhere, but it is not where bodies live. [...] Your legal concepts of property, expression, identity, movement, and context do not apply to us. [...] Our identities may

> "It is generally recognized that there is a need for legal regulation for many of the things done online."

32. In re Search Warrants Nos 16-960-M-01 and 16-1061-M to Google, para 25.

33. Australian government. (2018). *Australia's Tech Future*. Retrieved from https://www.industry.gov.au/sites/default/files/2018-12/australias-tech-future.pdf.

34. Software One. *Managing and understanding on-premises and cloud spend*. Retrieved from https://www.softwareone.com/on-premises-and-cloud-spend-survey/.

35. See e.g., European Commission. *Digital Single Market: Cloud Computing*. Retrieved from https://ec.europa.eu/digital-single-market/en/cloud.

36. Johnson, D.R. & Post, D.G. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, 48, 1367; Reidenberg, J.R. (1998). Lex Informatica. *Texas Law Review*, 76(3), 553; Geist, M. (2001). *Is there a there there? Towards greater certainty for internet jurisdiction*. Berkeley Technology Law Journal, 16, 1345; Menthe, D.C. (1998). *Jurisdiction in cyberspace: A theory of international spaces. Michigan Technology Law Review*, 4(1), 69; and Goldsmith, J.L. (1998). *Against cyberanarchy*. University of Chicago Law Review, 65(4), 1250.

be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose."[37]

While some of these thoughts may seem to belong to a bygone era today, other aspects are clearly still relevant – perhaps more as an explanation of the regulatory issues the ecosystem still faces today, rather than a manifesto. Sovereignty and enforcement remain complex and controversial issues. Cyberspace may be less 'borderless' now than it was then, but the clash between laws grounded in territoriality and a *prima facie* borderless, virtually global internet remains. Furthermore, some legal concepts are still difficult to transpose onto the online environment.

Nevertheless, questions of whether it is possible (or desirable) to regulate cyberspace are now 'dead issues'. It is generally recognized that there is a need for legal regulation for many online activities. For example, few would accept the idea of an online environment where laws against child abuse-materials do not apply. Consumers are less likely to engage in e-commerce if they are not afforded protection, and data privacy protection is at least as important online as it is offline. The fact that legal regulation plays an important role online is an important overarching meta-trend that affects every aspect of the topical trends, and the legal and technical approaches.

Nevertheless, the areas in relation to which the ecosystem relies on legal regulation are not necessarily static. As discussed in more detail below, while law is largely relied upon to create trust in online commercial transactions today, blockchain-based smart contracts may increasingly act as a competitor in some areas – even if the law remains an underlying facilitator of the trust created by smart contracts.

Meanwhile, while the applicability of law online is now firmly established, the era of so-called self-regulation is by no means over. Ultimately, regulating the internet requires a steady hand and a dispassionate mind. History has already proven that both inaction and over-action may be harmful for this sensitive and indeed fragile environment.

Self-regulation

Self-regulation has played a major role in the development of the internet and can occur on a variety of levels, ranging from infrastructure governance to peer-driven content moderation within a specific online forum. The domain name system is often cited as a prime example of successful self-regulation. As another example, one interviewed expert cited the self-regulation of counter-terrorism measures on the internet, as opposed to externally imposed rules. More broadly, another interviewed expert stressed the need for international agreement on standards of jurisdiction on the internet, because while companies should be encouraged to self-regulate, governments need to take responsibility, as well.

It is possible, however, that the wind is changing on self-regulation of companies (even in the US). Indeed, ICANN today could be seen as more of a hybrid organization, as governments play an increased role in its regulation.

2.2.2

Proliferation of initiatives

A plethora of new initiatives from public and private actors around the world have been announced or adopted to address the issues at stake. These include new national laws, codes of conduct, multilateral agreements and company policies. Many of these initiatives are discussed in the Chapter that outlines key topical trends, and in the Chapter that analyzes a range of legal and technical approaches.

Intensive developments on cross-border legal challenges online signal that these issues are now taken seriously, which is certainly important. Yet uncoordinated patching actions, taken in a reactive mode under the pressure of urgency, create a legal arms race with potentially detrimental impacts. Ensuring that the multiplication of different regimes does not create additional tensions, or even conflicts, is a major challenge.

The degree to which states seek to apply their laws to internet activities has not been static over the years. In fact, it is possible to identify a pattern of pendulum swings between what may be described as jurisdictional under-regulation on one side, and jurisdictional over-regulation on the other.[38]

Today, the regulatory environment is clearly swinging toward jurisdictional over-regulation. Indeed, the appetite with which states are now seeking to extend their jurisdiction and apply their laws to internet activities is unprecedented. Thus, one may speak of this as an era of jurisdictional 'hyper-regulation' characterized by the following conditions:

1. the complexity of a party's contextual legal system (i.e., the combination of all laws that purport to apply to that party in a given matter) amounts to an insurmountable obstacle to legal compliance; and

37. Barlow, J.P. (1996). A declaration of the independence of cyberspace. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/cyberspace-independence.

38. See further: Svantesson, D. (2017). *Solving the internet jurisdiction puzzle.* Oxford, United Kingdom: Oxford University Press, pp. 91-112.

2. the risk of legal enforcement of (at least parts of) the laws that make up the contextual legal system is more than a theoretical possibility.

One interviewed expert emphasized that governments are now seeking to control the online environment, which results in the creation of more laws, as their typical response is to introduce new laws rather than apply existing laws to confront the challenges.

A related trend is the fast pace at which political agendas and policy focuses change. For example, various online issues that gained limited attention just some years ago, such as online bullying, the spread of hate speech and non-consensual distribution of sexually explicit content, are now widely recognized as problems. The constant shifting of priorities and attention from one topic to another, often spurred by the news media, creates a sense of urgency that leaves governments with insufficient time to decide on or coordinate approaches.

2.2.3

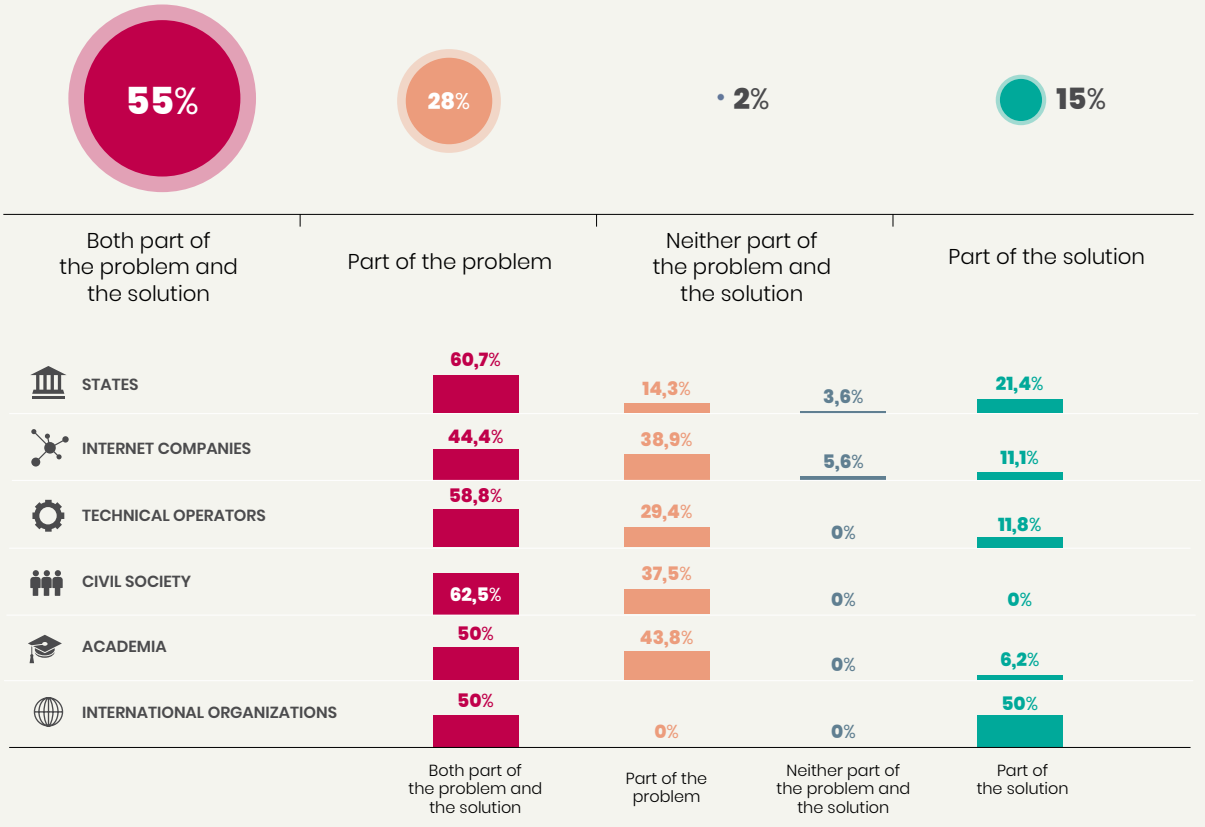
An increasing appetite to regulate cyberspace

Some interviewed experts noted that although governments in the past largely took the view that internet regulation was difficult or impossible, the political will to regulate the internet is now stronger than ever.

Just over half of surveyed experts indicated that they see this development as both part of the problem and part of the solution. In more detail, 55 % indicated that the increase in the enforcement of national laws in cases involving servers, users or companies located in other countries is both part of the problem and part of the solution. 28% saw it as just part of the problem, while 15% saw it as just part of the solution. 2% saw the increase in the enforcement of national laws in cases involving servers, users or companies located in other countries as being neither part of the problem nor part of the solution.

INFOGRAPHIC 10

Increased regulation of cyberspace: problem or solution?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

In their comments, surveyed experts expressed concerns around the increased enforcement of national laws in cases involving servers, users or companies located in other countries. In particular, surveyed experts pointed to concerns about arbitrariness, uncertainty, unintended consequences, inappropriate impact in third-countries, and a tension between state priorities and a global vision. Others noted that while adherence to treaties would be ideal, in its absence, extraterritorial national laws – if properly implemented – are a sensible interim solution. Some also argued that unilateral attempts highlight weaknesses in existing regimes, and as such, work as an inevitable catalyst for long-term change.

There were clear sectoral differences on this survey question, with stakeholders from the government sector and international organizations being considerably more positive about this development.

2.2.4

Information overload and accessibility

To move forward on the cross-border legal challenges on the internet in the most successful way possible, all stakeholders must have access to relevant information. Indeed, this is one of the reasons for this Report. The need for capacity building was a recurring theme in comments from surveyed and interviewed experts, and it is relevant in this context, as well. For example, one interviewed expert commented on the importance of developing a new way to educate policy makers, regulators and others so that the discussion remains robust in terms of legal tradition, but in a way that can be readily understood to prevent these stakeholders from 'switching off'. Interviewed experts from the tech sector made similar comments on capacity building, with some stressing the need for legislators and law enforcement to understand the technology and terminology.

Some interviewed experts pointed to the strong dominance of the English language as a current problem in the context of accessing information, noting that the cost of translations is a limiting factor. However, it was also noted that this current barrier is likely to decline, as younger generations in many states have high levels of English proficiency. One interviewed expert made the important observation that materials only being available in a foreign language forces reliance on brief secondary sources, which often lack nuance and are written for a generalist audience. This reality plagues all stakeholder groups and is also legitimate concern in relation to some of the materials relied upon for this Report.

One surveyed expert stated that information was accessed mainly on a regional scale. Another noted that although there is substantial information available about decisions in the US and Europe, there is not much information about decisions and developments in other states – including their rationale, their laws and the interpretation of those laws. This could be seen as a call for states around the world to do more to provide and promote free online access to their laws and court decisions, preferably with key developments accessible in multiple languages.

This observation is also of interest in relation to the widespread lack of issues and examples from other regions (outside the EU and US) in discussions of cross-border legal challenges on the internet – a problem strongly emphasized by numerous interviewed and surveyed experts. Surveyed and interviewed experts noted that much is being done to ensure regional diversity in the discussions, including greater representation from developing countries. Yet one may reasonably assume that part of the problem stems from EU/US developments becoming the common denominator in the discussions, partly due to their accessibility. As a result, these developments garner greater attention at the expense of examples from other regions, even when those regions are represented in discussions.

> "To move forward on the cross-border legal challenges on the internet in the most successful way possible, all stakeholders must have access to relevant information."

Variance in access to materials from different regions

Numerous surveyed and interviewed experts pointed to the **I&J Retrospect Database** of the Internet & Jurisdiction Policy Network as a leading source of information on the relevant actors and initiatives, the details of relevant laws and their application, as well as the relevant court decisions in the topic of cross-border legal challenges on the internet.
However, the wide variance in access to materials from different regions is also reflected in the Internet & Jurisdiction Policy Network's Retrospect Database.[39] For example, an examination of the reported cases during the year of 2018 – 240 in total – reveal the following statistics:

- 95 of these deal exclusively with Europe, and another 12 involve Europe plus at least one other jurisdiction;
- 28 cases deal exclusively with North America, and another 12 involve North America plus at least one other jurisdiction;
- 19 cases are geographically neutral;
- 17 cases deal exclusively with Asia (apart from China, India and Russia), and another 1 involves Asia (apart from China, India and Russia) plus at least one other jurisdiction;
- 14 cases deal exclusively with Russia, and another 1 involves Russia plus at least one other jurisdiction;
- 10 cases deal exclusively with India, and another 1 involves India plus at least one other jurisdiction;
- 9 cases deal exclusively with South America, and another 2 involve South America plus at least one other jurisdiction;
- 8 cases deal exclusively with Australia/New Zealand, and another 2 involve Australia/New Zealand plus at least one other jurisdiction;
- 9 cases deal exclusively with China;
- 9 cases deal exclusively with Africa; and
- 7 cases deal exclusively with the Middle East, and another 1 involves the Middle East plus at least one other jurisdiction.

While the Internet & Jurisdiction Policy Network's Retrospect database is clearly intended to capture information from around the world, the dominance of European materials is nevertheless overwhelming. This highlights the need for more and better information sharing, and points to the usefulness of future regional reports.

In this context, it is worth emphasizing the point that information sharing equals impact. For example, if a person from South America meets someone from Asia and neither knows much about the other's laws and approaches, but both have a basic understanding of European and North American approaches, they are perhaps likely to base their discussion on the common knowledge they share. This results in a 'disproportionate' influence of European and North American law, which is a key issue for both capacity building and inclusiveness.

2.2.5

Every problem has a solution, but every solution has a problem

While one may argue that judicial and legislative creativity has declined over recent years, some solutions have been advanced to address the complications regarding the establishment of a court's personal jurisdiction over a defendant in another territory. Many will recall, for example, the 'sliding scale' test articulated by US courts in the mid-1990s, which sought to organize websites by reference to their 'interactivity'.[40] And in the famous High Court of Australia case in 2002 between US publishing company Dow Jones and Victorian businessman Gutnick – which marked the first time that the highest court of any state considered the matter of jurisdiction over cross-border internet defamation – Justice Kirby determined that the solution was found in the doctrine of *forum non conveniens*.[41]
These solutions, like many others, have not stood the test of time. But the judicial self-restraint that Justice Kirby anticipated in the form of *forum non conveniens* is still frequently cited as a

39. Internet & Jurisdiction Policy Network. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect
40. Zippo Manufacturing Company v Zippo Dot Com, Inc 952 F.Supp 1119 (WD Pa 1997).
41. Dow Jones & Company Inc v Gutnick (2002) 210 CLR 575. For a recent discussion of the doctrine of *forum non conveniens* in relation to the internet, see: Haaretz.com v. Goldhar, 2018 SCC 28, 2018 2 S.C.R. 3.

potential solution, even though court attitudes toward jurisdiction appear to be moving away from self-restraint. Few proposed solutions are therefore truly 'new', and focusing on whether they are or not is arguably not the most fruitful approach. More important is how well a given solution addresses the concerns at hand.

The reality is that jurisdictional issues both online and offline are complex, and in light of the attempts at finding solutions so far, it seems clear that perfect solutions are improbable; indeed, the search for perfection can become an obstacle to progress. And given that the world is increasingly characterized by complexity, arriving at an all-encompassing international treaty to solve the myriad cross-border legal challenges online is highly unlikely within the foreseeable and even distant future.

Rather than waiting for the problems to go away, or to be resolved through an unlikely international treaty, stakeholders need to continue working on many different fronts, and ensure that their work is as coordinated as possible. Such work should also be grounded in solid conceptual frameworks – a component that is typically provided by academic research.

Yet despite the central role that the internet plays in modern society, and despite its increasing prominence in policy discussions, cross-border legal challenges on the internet are still treated as fringe issues in legal academic literature – not least within the fields of public and private international law. This is untenable. Cross-border internet-related legal issues are central matters in society today, and this must be reflected in public and private international law discussions.

Regrettably, it appears that the legal issues of internet jurisdiction are receiving less attention in legal academic literature.

Jurisdictional issues represent a decreasing proportion of academic work

Year	1994-1998	1999-2003	2004-2008	2009-2013	2014-2018
Number of journal articles addressing the legal issues of internet jurisdiction[42]	841	1,997	1,451	1,501	1,281
Number of journal articles addressing the internet[43]	13,762	31,646	34,680	39,392	37,981
Percentage of journal articles addressing the legal issues of internet jurisdiction out of total number of journal articles addressing the internet	6.1%	6.3%	4.2%	3.8%	3.4%

42. This study is based on a text search for journal articles either containing at least one sentence with both the term "internet" and the term "jurisdiction", or at least one sentence with both the term "Cyberspace" and the term "jurisdiction" (i.e. (Cyberspace /s jurisdiction) OR (Internet /s jurisdiction)). The searches were carried out on 7 January 2019 on the Law Journal Library of HeinOnline. The search was limited to the following categories: "Articles", "Comments", "Notes" and "Editorials", and included "external articles (articles outside of HeinOnline)" as well as "periodical results from other HeinOnline Collections". This approach admittedly has its limitations. Nevertheless, the result is indicative of the development in academic law journal articles, comments, notes and editorials addressing the topic of internet jurisdiction.

43. Result produced via the following search: (Cyberspace OR Internet). The searches were carried out on 7 January 2019 on the Law Journal Library of HeinOnline. The search was limited to the following categories: "Articles", "Comments", "Notes" and "Editorials", and included "external articles (articles outside of HeinOnline)" as well as "periodical results from other HeinOnline Collections".

Cross-border legal challenges arise within virtually all areas of substantive law and are often approached and debated within the context of each area. For example, these challenges may be discussed in the context of reforming intellectual property law, defamation law, cybercrime or taxation.

Yet it is also important to recognize that one can approach the cross-border legal challenges on the internet as a topic in its own right, and not merely as a component of different substantive law areas. Doing so reveals the extent to which identical or similar jurisdictional challenges arise in different settings, allowing solutions and approaches from one context to be transposed to another. More such 'meta-level' work is needed in this area.

2.2.6

Legal uncertainy increases

The activities of both natural persons (individuals) and legal persons (companies and other organizations) are regulated by law. In the offline environment, it is typically quite easy to identify the applicable law. For example, a person driving a car on roads in Germany is subject to German traffic rules. Identifying the applicable law(s) online is often more complicated.

When sending an email from Argentina to Japan, for example, a person may be subject to both the laws of Argentina and those of Japan. However, when the same person in Argentina posts a defamatory comment about a person in Finland to a social media site, she may be subject to not only the laws of Argentina and Finland, but the laws of all the countries in which she has contacts in her social media network – and perhaps any law specified in her agreement with the social media platform. As this example shows, it is important to bear in mind that applicable laws are determined by the activities we undertake.

To understand the complications that arise, it is useful to think of the laws that apply to a person in a given situation as a 'contextual legal system' – that is, a system of legal rules from different states that all apply to the activity undertaken by that person. It is then clear that, in the example involving an email sent from Argentina to Japan, the contextual legal system is less complex (because it consists of the legal rules of two states) than that of the latter example involving a defamatory social media posting.

A serious problem online is that people are often unable to predict all the states' laws that form part of their contextual legal system for any given activity. Even when a person can ascertain which states' laws apply to them, it is not always easy to access all those laws. Indeed, even where access can be ensured, language issues may mitigate a full understanding of those laws. In addition, the legal rules of a domestic legal system are typically structured to avoid situations where one legal rule demands something that another legal rule prohibits. However, where a contextual legal system consists of legal rules from different states – as is typically the case in relation to online activities – no such coordination can be presumed. As a result, it is not uncommon, online, for one legal rule within a relevant contextual legal system to require something that another legal rule within the same system prohibits. This lack of legal harmonization, while natural in light of how the world is organized, is a major hurdle, as it creates an environment in which ensuring legal compliance is difficult, or even impossible.

This poses obvious practical challenges. On a deeper level, it also undermines the legitimacy of at least one fundamental legal principle: the principle that ignorance of the law excuses not ('*Ignorantia juris non excusat*'), which is a cornerstone of any functioning legal system. If one acknowledges that the regulatory environment online makes it frequently impossible to be informed of one's legal obligations, it is difficult to maintain that ignorance of the law is no excuse. For now, the general impossibility of knowing all the laws that purport to apply, and the fact that ignorance of the law is typically no excuse, seem irreconcilable, affecting both the topical trends, and the legal and technical approaches.

"A serious problem online is that people are often unable to predict all the states' laws that form part of their contextual legal system for any given activity. Even when a person can ascertain which states' laws apply to them, it is not always easy to access all those laws."

2.3

Rethinking the role of territoriality

In relation to the matter of jurisdiction, territoriality is essentially meant to fulfil two functions. The first is to provide a criterion for when a state can claim jurisdiction. Online, however, it is particularly easy to find territorial anchor-points for jurisdictional claims. The second function of territoriality is to act as a 'stop sign' that provides a warning when one enters the exclusive domain of another state.

Here again, though, territoriality fails online. It is simply unrealistic to think that a state will be connected to the global community and still enjoy traditional exclusiveness, in the Westphalian sense.

In fact, it seems increasingly obvious that drawing a distinction between territorial and extraterritorial jurisdictional claims is misguided. This is because:

1. There is no (international) agreement on when a claim of jurisdiction is extraterritorial (which, assuming that extraterritorial is the opposite of territorial, logically precludes any agreement on when a claim of jurisdiction is territorial); and
2. Some 'extraterritorial' claims of jurisdiction are clearly supported in international law, as is the case, for example, under the nationality principle. In fact, exceptions to a strict adherence to territoriality are now so numerous that territoriality can no longer be seen as the jurisprudential foundation for jurisdiction.

Even where a jurisdictional rule is drafted in terms of territorial criteria, its true underlying aim is to establish whether the state making the jurisdictional claim has a sufficiently strong connection to the matter to create a legitimate interest in claiming jurisdiction; a territorial criterion is merely a proxy for this underlying aim. For example, while Article 3 of the GDPR purports to delineate the GDPR's scope of application in a spatial sense, it actually does so in a manner that is both territoriality-dependent and territoriality-independent. Thus, to speak of extraterritoriality is akin to describing cars as 'horseless carriages' – both descriptions are founded in a mistaken notion of what is 'normal'. Although the term is still used for the sake of convenience, we must be aware that extraterritoriality, as a concept, has been discredited.[44]

It is well established and beyond intelligent dispute that international law's focus on territoriality is a bad fit with the fluidity of the online environment, which is characterized by constant and substantial cross-border interaction. Yet until recently, little had been done, and even less achieved, in the pursuit of disentangling internet jurisdiction from territoriality.

In policy documents and academic writings, the most commonly cited source for a territoriality focus is the classic *Lotus case*[45], which was decided by the then-Permanent Court of International Justice in 1927. This case involved a collision between two steamships.

While principles articulated in one setting may legitimately be applied to cases in other settings, cases concerning colliding steamships clearly differ from those in the context of internet jurisdiction. Given that general legal methods call for treating different cases differently, there seems to be little point in grounding our thinking on internet jurisdiction in the *Lotus* decision. In fact, the majority opinion in *Lotus* emphasized the need to focus on "precedents offering a close analogy to the case under consideration; for it is only from precedents of this nature that the existence of a general principle applicable to the particular case may appear."[46]

Perhaps the real reason that the *Lotus* decision still receives so much attention is the fact that there are so few other international decisions on this topic. Rather than conceding that the

> "Rather than conceding that the absence of relevant case law means that this is an unsettled area of law, there has been a tendency to inappropriately overemphasize the *Lotus* decision."

44. See further: Ryngaert, C. (2015) *Jurisdiction in International Law 2nd edn.* Oxford, United Kingdom: Oxford University Press, p. 8.
45. Case of the S.S. "Lotus" (France v. Turkey), PCIJ Series A, No. 10, p. 21.
46. Case of the S.S. "Lotus" (France v. Turkey), PCIJ Series A, No. 10, p. 21.

absence of relevant case law means that this is an unsettled area of law, there has been a tendency to inappropriately overemphasize the *Lotus* decision.

Moreover, the *Lotus* judgment is not a particularly solid foundation for the territoriality principle, because it contains contradictions and lacks clarity in some areas. It is also a decision in which no less than half of the members of the court expressed a dissenting opinion, and there is not even any agreement as to what type of jurisdiction – prescriptive, judicial or enforcement – the *Lotus* case involved.

As the role of strict territoriality declines in the context of jurisdiction, something else must take its place as the jurisprudential core of jurisdictional claims. In the context of law enforcement access to digital evidence, at least, there are signs of an emerging consensus to focus on whether the state claiming jurisdiction has a legitimate interest and a substantial connection to the matter at hand, combined with an assessment of the consideration of other interests.[47] Discussions regarding the cross-border legal issues associated with law enforcement access to digital evidence are relatively advanced, and as one interviewed expert noted, this field is a major driver in cross-border legal issues. Reliance on this three-factor framework may therefore spread, as it can also be applied in other settings in which standards need to be imposed on claims of jurisdiction.[48]

Focusing on whether the state claiming jurisdiction has a legitimate interest and a substantial connection to the matter at hand, combined with an assessment of the consideration of other interests, has the advantage of incorporating a wide range of complex international law concepts, while also being easily understandable. This user-friendliness makes it an effective tool to overcome some of the 'artificial regulatory challenges' associated with cross-border legal issues on the internet. It further benefits from being relevant for both matters that traditionally fall within public international law and those that traditionally fall within private international law (or conflict of laws).

2.3.1

An increasing geographic reach of national laws

When jurisdictional rules are broad in scope, they risk capturing conduct with which there is an insufficient degree of contact to justify a state's jurisdictional claim. This may lead to jurisdiction being exercised over parties that lack adequate notice. At the same time, when jurisdictional rules are narrow in scope, they risk leaving victims without judicial redress. Striking the right balance is no easy task, and focusing on distinctions between territoriality and extraterritoriality frequently leads to both of these problems.

Many states make broad claims of jurisdiction over internet activities – claims that they cannot possibly back up with effective enforcement. While common, such 'jurisdictional trawling' is often a destructive regulatory approach, especially when it leads to arbitrary enforcement, which, as interviewed experts emphasized, is a poor fit with the rule of law.

In addition, as states compete to have their laws respected, many are increasing the potential fines for those who fail to comply. This is problematic in instances where compliance with one state's law necessitates the violation of another state's law.

The aforementioned 'jurisdictional trawling' and high potential fines are merely two examples of states flexing their muscles in relation to the internet. Comparing the issue of jurisdiction online and offline, arguably the biggest difference is that for online jurisdiction, there is a greater need to link the question of whether a claim of jurisdiction is appropriate with the question of over what jurisdiction is asserted. Put differently, it is harder in the online context to determine which aspects of a legal or natural person's activity are captured by a claim of jurisdiction and which are not. This is a topic that has so far gained little attention, and there is a clear need for more sophisticated tools to ensure that claims of jurisdiction are not broader than necessary to accomplish lawmakers' goals.[49]

Yet perhaps the biggest challenge relates to trying to change attitudes. Too

---

47. These 'other interests' may include the interests of individuals, see e.g., the work of Ireland-Piper regarding whether the 'abuse of rights' doctrine might be helpful in seeking to maintain an appropriate balance between the rights of states and of individuals (Ireland-Piper, D. (2017) *Accountability in Extraterritoriality*. Cheltenham, Edward Elgar).

48. See further: Svantesson, D. (2017). *Solving the internet jurisdiction puzzle*. Oxford, United Kingdom: Oxford University Press, pp. 57-90.

49. For examples of attempts at constructing such tools, see e.g., Svantesson, D. (2013). A 'layered approach' to the extraterritoriality of data privacy laws. *International Data Privacy Law*, 3(4), 278-286; and Svantesson, D. (2017). *Solving the internet jurisdiction puzzle*. Oxford, United Kingdom: Oxford University Press, pp. 171-189 outlining a framework for 'scope of jurisdiction'.

often, the aim of the rules of jurisdiction is understood to merely be to further the policy objectives of relevant substantive laws. For example, if defamation law aims to protect the reputation of individuals, the aim of relevant jurisdictional rules is perceived to be to make the substantive defamation law as widely enforceable as possible by extending the claim of jurisdiction globally. But this is too simplistic. The underlying role of rules of jurisdiction must always be to seek the effective enforcement of the relevant substantive law, while at the same time minimizing, or even avoiding, the risk of international tension and conflict.

2.3.2

Challenges of enforceability

It is easy to understand why states want their laws to be respected online in the same way they are respected offline. Indeed, as the world is structured today, each state may be understood to have the right to dictate what is available online in that state. At the same time, despite the obvious legitimacy of their ambition for online and offline legal parity, there are several other considerations that should be part of the equation.

First, merely claiming that a state's laws apply worldwide online does not make it so. International law imposes some restrictions – albeit vague ones – on when a state can claim that its laws apply. Furthermore, a state's ability to enforce its laws is often more limited than the claims it makes regarding the reach of its laws.

Second, as states make broader jurisdictional claims, they may become increasingly dependent on the cooperation of other states for the enforcement of those claims. Therefore, although broader claims of jurisdiction may lead to obvious clashes in some cases, they may also encourage greater cooperation and coordination among states.

Any potential positive impact of broader jurisdictional claims may be lost when states are content to limit themselves to what may be termed 'domestic enforcement of extraterritorial claims'. Rather than relying on enforcement through the cooperation by a foreign state, states, in this scenario impose 'market destroying measures' on the foreign party, such as restricting that party's access to users in the country in question.[50] Such exercises of 'market sovereignty' are seemingly increasing in frequency.

Third, where a state makes the claim that its laws apply to certain online activities, it needs to be prepared to accept equally broad claims from other states.

Fourth, jurisdictional hyper-regulation imposes a significant cost of compliance on all natural and legal persons who seek to abide by all applicable laws.

Fifth, there is a risk that natural and legal persons who seek to abide by all applicable laws adhere to the strictest standards, under the logic that compliance with the strictest standards ensures compliance with all relevant laws. Such a 'race to the bottom' may have irreversible consequences for diversity online.

Taken together, these considerations suggest that the legitimate aim of having state laws respected online in the same way as offline must be pursued in a careful and intelligent manner. In our current era of jurisdictional hyper-regulation, there is a clear meta-trend of states making overly broad and unsophisticated claims of jurisdiction where more limited, intelligent and nuanced claims of jurisdiction would:

1. be easier to defend both morally and under international law;
2. be easier to enforce;
3. impose lower compliance costs; and
4. be less likely to encourage overly broad claims of jurisdiction by other states.

> "As states make broader jurisdictional claims, they may become increasingly dependent on the cooperation of other states for the enforcement of those claims. Therefore, although broader claims of jurisdiction may lead to obvious clashes in some cases, they may also encourage greater cooperation and coordination among states."

50. See further: Svantesson, D. (2016). *Private international law and the internet* (3rd ed.). Alphen aan den Rijn, The Netherlands: Kluwer Law International, pp. 11-12.

2.3.3

When territoriality is irrelevant

Given the above, it is only natural that we have seen a slow but steady decline in the focus on territoriality for jurisdictional purposes. As discussed in a later Chapter, some recent examples of this include the 2018 US CLOUD Act; the EU's *Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*[51]; and the EU's *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*.[52] Further, Article 3(1) of the EU's GDPR specifically emphasizes that the location of data processing is irrelevant. With these instruments, the EU and US are shifting their focus away from the location of the data in question, and from territoriality more broadly.

The shift away from blind adherence to territoriality as the foundation of jurisdiction must be understood in light of the fact that territoriality-based thinking encourages data localization, and fragmentation more broadly. Furthermore, territoriality, as a concept, suffers from several weaknesses, especially when applied in online contexts where determining the location of a specific activity necessitates entering the quagmire of legal fictions.

At the same time, it should be noted that difficulties in applying the concept of territoriality are by no means limited to the online environment. Such difficulties are also common offline, particularly in fields such as human rights law, aviation law and anti-competition law. It is time to recognize that what are normally discussed as 'exceptions' to the territoriality principle are too numerous, and too important, to be seen as mere exceptions. These exceptions must instead be recognized for what they really are: indicators that jurisdiction, as a jurisprudential concept, is not rooted in territoriality.

> "Jurisdiction, as a jurisprudential concept, is not rooted in territoriality."

2.4

Normative plurality, convergence and cross-fertilization

It is a well-established fact that law is not the only factor affecting conduct online.[53] Indeed, law does not always have the greatest effect on conduct online. This has profound implications.

2.4.1

Blurring of categories

Interviewed experts noted that there is sometimes a fine line between legitimate political speech on the one hand, and hate speech or defamatory content on the other. Some measures aimed at removing the latter risk suppressing the former. One interviewed expert also observed that there is no broad agreement on norms, behaviors and types of content that are universally acceptable. The international differences are great; content may be classified as hate speech in one jurisdiction, for example, while it may be classified as acceptable in another. Interviewed experts underscored this point by drawing a comparison between how the US and Germany treat hate speech.

In a 2012 Report, the UN Special Rapporteur on Freedom of Expression

51. COM(2018) 226 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=EN.
52. COM(2018) 225 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN.
53. See e.g.: Lessig, L. (1999). The law of the horse: What cyberlaw might teach. Harvard Law Review 113(506).

pointed to three different types of expression: (1) expression that constitutes an offense under international law and can be prosecuted criminally; (2) expression that is not criminally punishable but may justify a restriction and a civil suit; and (3) expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others. This remains a useful categorization, and as noted by the Special Rapporteur, these categories of expression pose different issues that call for different legal and policy responses.[54]

If these categories are not taken into consideration, distinctions between illegal content, content that is contrary to terms of service and objectionable content may become blurred. Such blurring must be avoided, especially given that, as affirmed by the UN Human Rights Committee, Article 19 of the *International Covenant on Civil and Political Rights* (ICCPR) protects the expression of opinions and ideas, even if some individuals may see them as deeply offensive.[55]

Drawing upon the aforementioned work, it may be possible to point to the following six types of expression:

The six types of expression:

1. Expression that constitutes an offense under international law and can be prosecuted criminally
2. Expression that constitutes an offense under national law and can be prosecuted criminally
3. Expression that is not criminally punishable but may justify a restriction and a civil suit
4. Expression that is not against applicable law, but violates relevant terms of service
5. Expression that is neither against applicable law, nor relevant terms of service, but seen by some as offensive
6. Expression that is entirely uncontroversial

It may be tempting to view this structure as a form of ranking. Doing so, however, involves at least one inappropriate simplification: not all laws are made equal. It is often argued that laws should trump terms of service, because whereas laws are the result of an established democratic process, the terms of service are unilaterally imposed by profit-driven corporations. This reasoning does not lack merit, but if the superior position of laws is founded upon their democratic pedigree, what about laws that are not based on democratic processes? What is, for example, the proper relationship between terms of service and dictatorial laws aimed at suppressing democratic movements?

2.4.2

Harmonization via company norms

Another notable overarching trend is the comparatively high degree of transnational harmonization through company norms, versus the fractured country-based norm setting and decision making. There is a considerable degree of harmonization across the norms (e.g., terms of use) implemented by the major (US-based) internet platforms. This may be explained, in part, by the fact that these platforms are subject to the same legal requirements from various states. But such harmonization clearly goes beyond those legal requirements, which suggests that it must be understood as being in the platforms' interest – even though the extent to which this harmonization may expand beyond dominant internet platforms remains to be seen.

The laws of different states, by contrast, are yet to reach a comparable degree of harmonization. Given how far-reaching cultural, economic, societal, and religious differences impact the fundamental laws of each state, such harmonization seems unlikely.

Interviewed experts also drew attention to the cooperative spirit among the major internet platforms in pur-

54. Annual report of the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression to the General Assembly. (2012). A/67/357, para. 2.

55. United Nations, Human Rights Committee. (2011, September 12). *General Comment No. 34 on Article 19: Freedoms of opinion and expression.* CCPR/C/GC/34, para 11.

suit of common goals, such as content moderation. As some interviewed experts noted, there is less of a cooperative spirit among states, aside from sectoral cooperation in the context, for example, of law enforcement. In fact, interviewed experts noted a clear trend of individualism among states, with each state prioritizing its own interest over the interest of the global community.

It is also noteworthy that, in relation to some types of content, platforms have taken the lead in setting standards. The move against non-consensual distribution of sexually explicit media is one example of this.

In an environment where standard creation is not the exclusive domain of nation states, these differences between harmonized company norms and fractured country-based norm setting may have long-term implications of strong relevance for cross-border legal challenges on the internet.

2.4.3

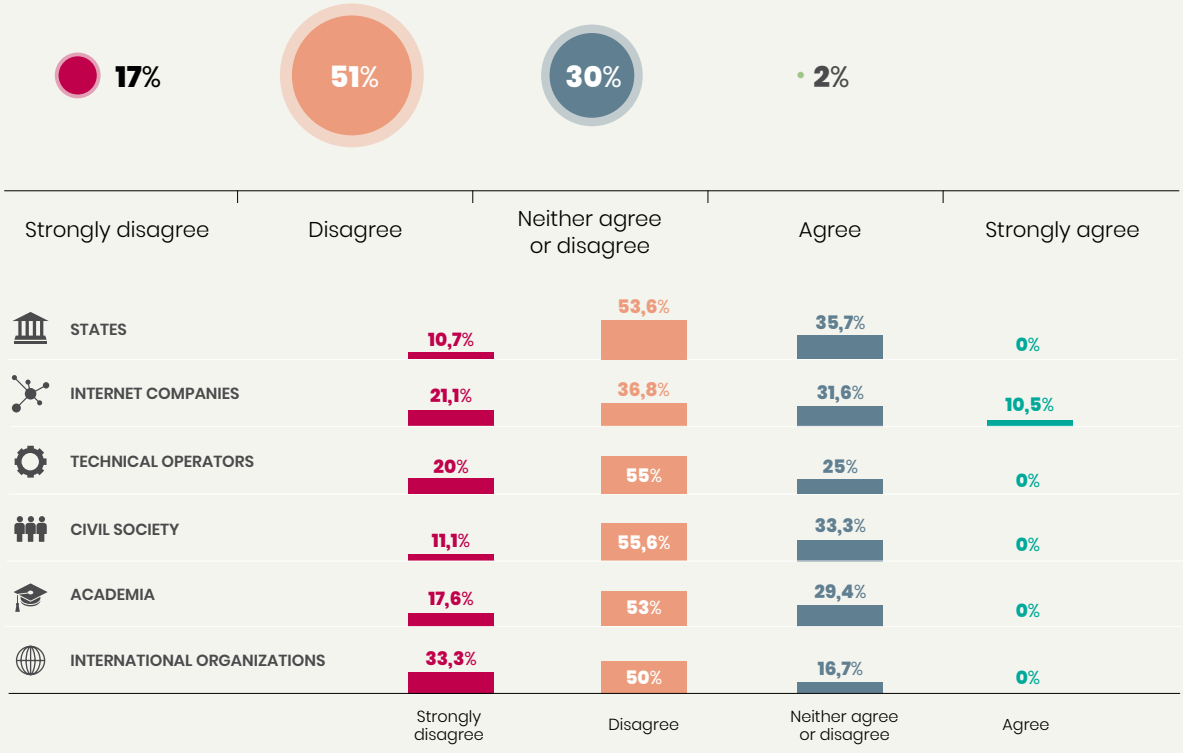
Judicial cross-fertilization – scalability, replication and imitation

The physical structure of the internet is coordinated to a large extent. Many aspects of the logical layer, such as the domain name sphere, are coordinated, as well. Yet both the literature and stakeholder input provided for this Report suggest that there is a lack of international coordination and cooperation on regulation of the internet more broadly.

A clear majority (68%) of surveyed experts 'strongly disagreed' or 'disagreed' that the existing tools of inter-state legal cooperation are effectively addressing online abuses. Only 2% 'agreed' or 'strongly agreed', while 30% responded that they 'neither agreed nor disagreed'.

INFOGRAPHIC 11

Do existing inter-state legal cooperation tools effectively address online abuse?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

The responses highlighted consensus across regions and stakeholder groups, and several important comments from surveyed experts substantiate concerns held throughout the ecosystem. For example, one surveyed expert noted that tools alone cannot address online abuses, and that effective mitigation xisting fundamental differences in state attitudes toward the roles that democracy and religion should play in legal matters further complicate efforts at coordination. Furthermore, several surveyed experts stressed that although existing tools of inter-state legal cooperation may be sufficient for non-urgent matters, slow bureaucratic procedures are a bad fit with the rapid pace of the internet.

In their comments on the existing tools of inter-state legal cooperation, surveyed experts also emphasized the need for a multistakeholder approach. For example, one comment noted that it is not only governments that need to work together, but business and civil society, as well. At the same time, several surveyed experts commented that although there is still a long way to go, improvements are noticeable.

This lack of coordination is a direct, and perhaps natural, consequence of the fact that states enjoy sovereignty insofar as they have the capacity to make their own laws. Given that states take fundamentally different approaches to matters such as balancing human rights, protecting consumers and supporting business, it is not surprising to see them face problems in coordinating internet regulation. Further complicating efforts at coordination are fundamental differences in state attitudes toward the roles that democracy and religion should play in legal matters. The complexity of this situation will only increase as more developing states play bigger roles online. As previously noted, the international climate has also changed more broadly in recent years, as states move away from international collaborative efforts and common goals, and toward more inward-looking policies that prioritize the immediate interests of each state. To put it simply, international distrust seems to be increasing. This broader political trend inevitably presents an additional hurdle for the effective coordination of internet regulation.

At the same time, it remains a fact that, due to the cross-border nature of the internet, the challenges faced online can only be addressed through international collaborative efforts and the pursuit of common goals; stakeholders simply cannot afford to not collaborate. An individual state neither can, nor should, control the internet or what is available online. For the moment, international multistakeholder dialogue remains the only alternative.

> "There are numerous indicators that the world is not ready for a general international agreement to settle all matters of internet regulation. Such a giant leap is unfortunately unrealistic."

However, there are numerous indicators that the world is not ready for a general international agreement to settle all matters of internet regulation. Such a giant leap is unfortunately unrealistic. Instead, progress will be achieved through many small steps, at least for now. States could increase efforts to identify uniting features and to iron out at least the most serious inconsistencies and clashes between domestic legal systems, in relation to both substantive and procedural law.

In this context, interviewed experts noted that although harmonization may be impossible on some topics at the moment, greater harmonization seems both possible and valuable on other topics (e.g., data breach notification schemes).

Hints of the 'small step' progress discussed above can be seen in the emergence of global jurisprudences via judicial cross-fertilization. Simply put, courts and regulators are increasingly heeding, copying and imitating approaches taken by foreign courts. Examples of this are prominent in the data privacy field, for example, where the EU's GDPR is being widely imitated.

As discussed in more detail below, judicial cross-fertilization is by no means occurring in an evenhanded manner. In many instances, the influence is unidirectional rather than mutual – typically from industrialized states to developing states.

More broadly, this judicial cross-fertilization acts as a 'double-edged sword'. In cases where the approach adopted from another court works toward increased international harmonization, imitating that approach may obviously have a positive impact. But in cases where the approach adopted from another court is aggressive in nature, each adoption of that approach into a new legal system moves us further from solutions to the cross-border issues faced online. Not all approaches are scalable, either. Courts and other lawmakers should always bear this in mind, both when selecting how they approach a specific legal issue, and when deciding which, if any, approaches from foreign courts or lawmakers to adopt.

In addition, courts and other lawmakers ought to bear in mind that the ultimate goal of international law is to help to ensure the survival of the human species, with obvious sub-goals such as ensuring peaceful coexistence, environmental protection and upholding human rights. The internet can play an important role in helping to build international links and relations through cross-border communication and interaction. We must therefore avoid using the online environment as a new arena for international conflict. These goals must be integrated into any assessment of internet jurisdiction.

2.4.4

Rules are set for – and by – established large actors

An examination of the survey and interview results points to five factors that, together, make a range of actors – developing countries, smaller countries and smaller internet actors – feel disempowered:

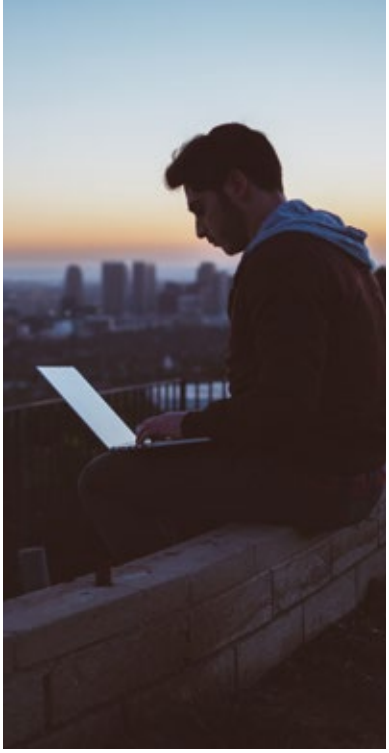
1. There is a perception that, compared to developed countries, developing countries have less of a say in the approaches taken by the major internet actors;
2. There is a perception that, compared to major internet actors, smaller internet actors have less of a say in the approaches taken by the regulators;
3. There is a perception that both smaller internet actors and developing countries lack a voice in the international dialogue;
4. Extraterritoriality allows dominant states to impose their laws on the world, while smaller states lack the standing and means to enforce their laws even domestically; and
5. Legal approaches from developed countries are being replicated to such a degree that it impactsthe sovereignty of developing countries.

A concern raised by several interviewed and surveyed experts is that much of the discussions around how to tackle the cross-border internet issues faced on the internet centers around the largest internet companies – particularly US-based companies such as Google, Microsoft, Facebook, Apple, Amazon, Twitter and eBay. There are non-Western examples of this dynamic, as well; Chinese standards, for instance, are introduced as a *de facto* component of subsidized mobile and terrestrial broadband infrastructure projects in parts of Africa. This leads to a skewed perspective of the issues faced by the great majority of internet actors, which consists of smaller businesses and organizations.

In fact, large actors may also be at a disadvantage in dialogues where they have a structure or business model that deviates from the more standardized structures of the major actors. For example, Wikipedia operates across borders and is available in different versions, like other major internet platforms. However, the various Wikipedia versions are language-based and independent from one another – which is distinctly different from the more standard approach of publishing different country versions of a platform. The implications of this structural difference are profound. In the context of content removal orders, for example, a court order to remove certain content will inevitably affect all users of the Wikipedia language version in question, and removal on one language version has no impact on what is available on another language version. Courts and regulators need to be alert to the legal implications of this type of structural differences.

There are obvious practical reasons for directing most attention at the major internet platforms. Where governments wish to maximize impact, they naturally target companies with the greatest number of users. And the major internet companies have the resources to participate in discussions on matters of internet regulation. Yet despite such practical justifications, the under-representation of smaller internet players remains an overarching meta-trend that ought to be addressed.

Highlighting a related meta-trend, many interviewed and surveyed experts from developing countries (and, to a degree, from smaller countries) perceived that they become aware of, and participate in, important policy and regulatory discussions only when many decisions have already been made. This is partially an issue of access to information, and is discussed in more detail elsewhere in this Report.



> "The under-representation of smaller internet actors and developing countries in crafting solutions requires both rethinking and restructuring."

There is a continuing need to work on solutions for soliciting and incorporating early input from all stakeholders. The under-representation of smaller internet actors and developing countries in crafting solutions requires both re-thinking and restructuring. Increased capacity building is one of the more obvious responses. There is also a power imbalance in the context of the extraterritorial application of laws. Some states have greater power to have their laws enforced in an extraterritorial manner, even in cases where the laws in question are identical, or near identical. This power imbalance – often between industrialized and developing countries – may become increasingly visible as more states adopt 'rep localization' requirements.

2.5

New roles for intermediaries

Without internet intermediaries such as search engines, auctioning platforms, video platforms and social media platforms, the internet would be considerably less useful, and considerably less user-friendly. Indeed, internet intermediaries play a central role in the operation of the online environment; they have in the past, they do so now, and they will continue to do so in the future. Yet their exact roles and responsibilities are contested and controversial topics, and the subject of significant work. The Stanford World Intermediary Liability Map, for example, is an online resource that provides internet platforms and others with information on online liability laws.[56]

2.5.1

Increasing responsibility bestowed on private operators

The increasing responsibility bestowed on private operators – through both laws that make internet platforms the gatekeepers of content and the voluntary assumption of responsibility – has occurred in numerous fields. This trend is particularly discernable in certain fields, and has evolved particularly far in the context of terrorism, extremism and hate speech – fields in which some laws demand fast response times in content blocking. For example, on December 19, 2018, Facebook announced that it had banned 425 pages, 17 groups, 135 Facebook accounts and 15 Instagram accounts for engaging in coordinated inauthentic behavior linked to the situation in Myanmar.[57] The banned accounts were sharing anti-Rohingya messages – the same kind of messages that have fueled a broader genocide in Myanmar.[58]

As far as extremism and hate speech are concerned, the most widely noted framework for increasing responsibility bestowed on private operators is the 2016 *Code of conduct on countering illegal hate speech online* presented by the EU Commission, together with Facebook, Microsoft, Twitter and YouTube. Under this arrangement, the mentioned IT companies undertake to:

- Have in place clear and effective processes to review notifications regarding illegal hate speech on their services so they can remove or disable access to such content.
- Have in place Rules or Community Guidelines clarifying that they prohibit the promotion of incitement to violence and hateful conduct.
- Upon receipt of a valid removal notification, review such requests against their rules and community guidelines and, where necessary, national laws transposing the Framework Decision 2008/913/JHA, with dedicated teams reviewing requests.
- Review the majority of valid notifications for removal of illegal hate speech in less than 24 hours and remove or disable access to such content, if necessary.

The cross-border implications are obvious.

---

56. Stanford Center for Internet and Society. (2018). *World Intermediary Liability Map*. Retrieved from https://wilmap.law.stanford.edu/.
57. Internet & Jurisdiction Policy Network. (2018, December). Facebook announces ban of over 400 pages and 100 accounts relating to Myanmar conflict. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7741_2018-12.
58. Wagner. K. (2018, December 18). Facebook removed hundreds more accounts linked to the Myanmar military for posting hate speech and attacks against ethnic minorities. *Recode*. Retrieved from https://www.recode.net/2018/12/18/18146967/facebook-myanmar-military-accounts-removed-rohingya-genocide.

2.5.2

(In)voluntary gatekeepers

The role of – and possible protection for – internet intermediaries is often approached from extremist points of view. Some seek to impose an uncompromising free speech regime, under which internet intermediaries impose no restrictions on what internet users upload. Others see internet intermediaries as little more than useful tools for government control of internet content and activities. Such extreme views are ultimately unhelpful, and we need to strive for an appropriate balance.

Historically, Western countries have viewed internet intermediaries as crucial for the development of the internet, and have therefore afforded them extensive protection – for example, in the form of the well-known §230 of the US *Communications Decency Act* of 1996 and through Articles 12-15 of the EU's *E-Commerce Directive*.[59] Both these instruments provide internet intermediaries with protection against liability in certain circumstances. But this attitude seems to be changing.

In focusing on cross-border legal challenges on the internet, four key issues must be addressed as a matter of urgency:

1. The need to minimize, or preferably eliminate, situations where internet intermediaries risk violating one state's law by complying with another state's law;
2. The need to clarify the extent to which internet intermediaries – as private actors – may assume the role of fulfilling quasi-judicial functions (either voluntarily or involuntarily);
3. The need to ensure that the law provides the clearest possible guidance as to what is expected of the internet intermediaries; and
4. The need for clear distinctions between situations where internet intermediaries are viewed as publishers and where they are seen as neutral platforms.

Situations where a party risks violating one state's law by complying with another state's law are referred to as 'true' conflicts of laws. There is widespread recognition that they benefit no one and should be avoided. The problem is finding a way to do so in a climate where states are rarely willing to compromise on the applicability of their laws.

Yet a potential model can be found in Australia's *Privacy Act*. Section 6A limits the extraterritorial effect of the Act by providing that: "[a]n act or practice does not breach an Australian Privacy Principle if: (a) the act is done, or the practice is engaged in, outside Australia and the external Territories; and (b) the act or practice is required by an applicable law of a foreign country."[60]

The duties-focused definition of conflicts of laws only describes part of the problem. There are also so-called 'false' conflicts of laws. These occur when a person subject to two or more laws can comply with all the applicable laws, which can be the case if one law is more flexible than the other, or if one law gives a right and the other imposes an opposing duty.

In the context of internet intermediaries, the importance of such 'false' conflicts of laws may be underappreciated. The correlative relationship between rights and duties, familiar to us from domestic law, does not exist in the cross-border environment; rights provided under one state's legal system may not necessarily create corresponding duties under other legal systems. To assess whether two (or more) laws are in conflict, we need to account for both the duties and the rights for which those laws provide. In other words, even where duties do not clash, but the rights of one country clash with the duties of another state, we need to carefully evaluate to which law priority is given. In an international context, there are no legal reasons for an internet intermediary to automatically prioritize duties imposed by one state over the rights afforded by other states. On a practical level, however, internet intermediaries may seek to avoid penalties by abiding by the duties imposed by one state rather than pursuing the rights afforded under the law of other states, unless they receive safeguards. This leads to a risk of over-blocking and a race to the bottom.[61]

Internet intermediaries fulfill quasi-judicial functions in a variety of contexts. Sometimes this happens voluntarily, and sometimes this role is forced upon them. Examples of the former include actions such as the removal of child abuse materials. For example, on October 24, 2018, Facebook announced that it had removed 8.7 million child abuse

> "Internet intermediaries fulfill quasi-judicial functions in a variety of contexts."

59. Directive (EC) 2000/ 31 of the European Parliament and Council, 8 June 2000, on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce [2000] OJ L178/ 1, 369.
60. Privacy Act 1988 (Cth) s 6A(4).
61. PwC. (2018). *Top policy trends of 2018*. Retrieved from https://www.pwc.com/us/en/risk-regulatory-consulting/assets/top-policy-trends-2018.pdf.

images in the previous three months, using previously undisclosed software that helps flag potential child abuse material for its reviewers.[62]

An observation made by one interviewed expert is particularly pertinent in this context. Perhaps due to the company structure commonly adopted by major US internet platforms, and perhaps out of convenience, decisions relating to content blocking and takedowns are often implemented on a regional, rather than national, basis in some parts of the world. For example, if one country in the Middle East orders content to be blocked or taken down due to blasphemy laws, that content is frequently blocked or removed for the entire region – even though the content in question may well be lawful in some countries in the region.

There are many examples of internet intermediaries being forced to assume a quasi-judicial function. For example, on December 6, 2018, Ugandan internet service providers (ISPs) started implementing a directive of the Uganda Communications Commission (UCC) to block access to websites with adult content;[63] examples from China, Indonesia, Korea, Russia, Turkey as well as Australia and the EU are mentioned later in the Report.

In these situations, internet intermediaries become the censors and gatekeepers of speech – a role for which they are typically ill suited. It is questionable whether society should assign such a crucial role to private entities.

Some may point to the fact that newspapers, radio and TV broadcasters have long acted as censors in deciding what content to make available. But the role of the internet intermediary is so fundamentally different that one cannot, and should not, draw such a comparison. A common argument holds that internet intermediaries are more like the postal service, passively distributing other people's content without interference. Yet such analogies may only serve as a distraction, rather than providing a useful tool for discussion. The reality is that no intermediaries in history have had to manage the volume of user-generated content that internet intermediaries do today.

The role of internet intermediaries must therefore be approached with fresh eyes, free from preconceived notions based on comparisons with the roles of offline intermediaries.

Expectations of internet intermediaries only serve to complicate the situation. While most people would expect internet intermediaries to abide by the law of their respective countries, they would probably not want them to abide by all laws of all other countries in the world. In the end, such compliance would force internet intermediaries to account for only the most restrictive laws from all the countries in the world. Such a 'race to the bottom' is certainly an unhealthy direction for the internet. And if this is undesired, there is a need to consider whether a globally active internet intermediary can ever be excused for not complying with all the laws around the world that claim to apply to its conduct. If stakeholders answer that question in the affirmative, how should a globally active internet intermediary decide which laws to abide by? These are, to a degree, novel questions in international law.

Without clear guidance from the law, internet intermediaries may be tasked with deciding the legality of certain content.[64] In such a situation, one could argue that internet intermediaries are set up to fail due to the vagueness of the laws they must apply. It may also be noted, in this context, that internet intermediaries are tasked with fulfilling such quasi-judicial functions at a fast pace, while the judiciary may take months or even years to reach a decision on the same matter.

Because it may be difficult to identify and bring to justice the party responsible for specific online activities, litigants and regulators may be tempted to target the internet intermediary used for those activities, instead. Justice Fenlon made this point very clearly in the aforementioned Canadian *Equustek* case, stating: "Google is an innocent bystander but it is unwittingly facilitating the defendants' ongoing breaches of this Court's orders. There is no other practical way for the defendants' website sales to be stopped."[65] Justice Fenlon's message is clear: where the legal system fails, internet intermediaries can expect to become the scapegoats of choice.

There is also a long-standing issue of distinguishing between internet intermediaries as publishers and internet intermediaries as neutral platforms. Obviously, protections for neutral platforms may not extend to situations where internet intermediaries act as publishers. This crucial neutrality is undermined when platforms are required to promote specific narratives, as was the case in the 2016 European Union *Code of Conduct* on countering illegal hate speech online. In this context, it has been noted that: "While the promotion of counter-narratives may be attractive in the face of 'extremist' or 'terrorist' content, pressure for such approaches runs the risk of transforming platforms into carriers of propaganda well beyond established areas of legitimate concern."[66]

---

62. Internet & Jurisdiction Policy Network. (2018, October). Facebook announces it has removed 8.7 million child abuse images in past three months thanks to previously undisclosed software. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7567_2018-10.

63. Internet & Jurisdiction Policy Network. (2018, December). Uganda: ISPs start implementing regulator's order to remove access to websites with adult content. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#article-7736_2018-12.

64. Sartor, G. (2013). Provider's liability and the right to be forgotten. In D. Svantesson & S. Greenstein (Eds.) *Nordic yearbook of law and informatics 2010– 2012: Internationalisation of law in the digital information society*. Copenhagen: Ex Tuto Publishing. 101– 37, 111.

65. Equustek Solutions Inc. v. Jack, 2014 BCSC 1063, para 156.

66. United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom and Expression. (2018) 2018 *Thematic Report to the Human Rights Council*. A/HRC/38/35. Retrieved from http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/35, p. 8.

One interviewed expert considered that through mergers, acquisitions and growth, many intermediaries are changing functions to the extent that within the same company, there may be an advertiser, brand holder, registrar and publisher, and that this creates an interesting tension. Another interviewed expert commented that intermediaries, particularly in geographically bounded spaces, are faced with many different jurisdictions and associated rules that pose a significant challenge – not only for their compliance with those rules, but for communicating how they apply those rules.

Yet another interviewed expert saw this aspect as leading to the vesting of significant power in those companies to implement solutions. That is, if these companies implement localized solutions on certain issues, it may lead to a more fragmented internet with different rules that apply in different places. This expert was concerned about the lack of ability for smaller players, including businesses and small countries, to influence the larger intermediaries in the implementation of policies. Indeed, as one interviewed expert stressed, this issue also extends to mid-level powers who enact policies that large platforms largely ignore, unless they fit with the current approaches of the biggest countries.

2.5.2

Appeals and recourse become key issues

When a court or an authority decides a matter, it is typically possible to appeal their decision, and to gain an insight into the reasoning that led to their decision. Such a transparent appeals mechanism is currently lacking in situations where a private actor acts as the decision maker. This is a serious consideration in a context where private operators have increased responsibility to act as filters of extremism and hate speech.

As one interviewed expert noted, the lack of grievance resolution mechanisms and the need for transparency among platforms are being discussed as part of the UN Internet Governance Forum's Dynamic Coalition on Platform Responsibility.[67] This expert noted that the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (Special Rapporteur on FOE) also recommended, in a 2018 Thematic Report to the United Nations Human Rights Council, that companies improve their transparency and accountability in content regulation.[68]

It should be noted that many of the larger internet companies issue transparency reports. But as observed by one interviewed expert, while those reports include aggregate numbers of content takedowns, they do not currently provide nuanced details about how decisions are being made.[69] On the topic of transparency, one interviewed expert said that companies have not successfully found a way to communicate the details of their internal procedures and how they apply different rules. This failure has provoked a normative backlash by governments, particularly in the context of hate speech and fake news.

The issue of accountability is receiving more attention, as well. The *Institute for Accountability in the Digital Age* (I4ADA), for example, was founded with the mission to ensure that online reaches of norms and values do not undermine the internet's potential to increase access to knowledge, spread global tolerance and understanding, and promote sustainable prosperity.[70] To that end, I4ADA is working on a set of principles – the *Hague Global Principles for Accountability in the Digital Age*[71] – with significant implications for the cross-border legal challenges on the internet.

---

67. Internet Governance Forum. *Dynamic Coalition on Platform Responsibility*. Retrieved from https://www.intgovforum.org/multilingual/content/dynamic-coalition-on-platform-responsibility-dcpr. See also initiatives such as: Internet Policy Observatory. The Santa Clara Principles on Transparency and Content Moderation. Retrieved from http://globalnetpolicy.org/wp-content/uploads/2018/05/Santa-Clara-Principles_final.pdf and Manila Principles on Intermediary Liability. Retrieved from https://www.manilaprinciples.org/.

68. United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom and Expression. (2018). *2018 Thematic Report to the Human Rights Council*. A/HRC/38/35. Retrieved from https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/ContentRegulation.aspx.

69. See further the work of: Ranking Digital Rights. Retrieved from https://rankingdigitalrights.org/.

70. Institute for Accountability in the Digital Age. Retrieved from https://i4ada.org/.

71. Institute for Accountability in the Digital Age. (2018). *The Hague Global Principles for Accountability in the Digital Age*. Retrieved from https://i4ada.org/#principles.

03

TOPICAL TRENDS

PREVIEW

On the occasion of the 14th United Nations Internet Governance Forum, full versions of Chapters 3 (Topical Trends), 4 (Legal and technical approaches) and 5 (Relevant concept clusters) will be launched that will supplement these initial Key Findings. Stakeholders from around the world will be invited between June-October 2019 to contribute online to the global data collection and mapping effort, adding to the input from more than 100 key stakeholders from five continents who contributed to the present Key Findings of the first edition of the Internet & Jurisdiction Global Status Report 2019.

The following sections provide a preview of the upcoming chapters and their preliminary table of contents.

Concerns regarding jurisdictional tensions in cyberspace are widespread, as the cross-border nature of the internet conflicts with the patchwork of territorially bound national laws. The high degree of legal uncertainty increases the cost of doing business, and challenges governments to protect their citizens and ensure respect of their laws.

It may also prevent internet users from accessing as broad a range of content as they otherwise could, and raises civil society concerns that abuses are not properly addressed, or that attempted solutions will harm users. Addressing these concerns is a matter of urgency.

To understand the details and full complexity of the cross-border legal challenges on the internet, it is useful to map out the major trends within the topics that are most relevant to the Internet & Jurisdiction Policy Network's stakeholder groups.

To this end, this Chapter will highlight a selection of particularly significant 'trends' within topics ranging from data privacy to taxation, and from the Internet of Things to cybercrime. These diverse topics have been grouped into three broader categories:

1. Expression
2. Security
3. Economy

While this approach should aid the clarity of the presentation, some topics may fit into more than one category. There are also obvious points of connection and indeed overlap across these categories. For example, economic interdependence among states remains a check on aggressive behavior[72], which highlights the link between security and economy.

Within each of the topics, more detailed attention is given to particularly important trends as identified through the survey results, interviews and extensive desk research, including an analysis of the Internet & Jurisdiction Policy Network's wide-ranging collection of relevant trends and developments available in the I&J Retrospect Database.[73]

These sources have also made it possible to briefly outline other significant trends within each topic area. The goal is to be comprehensive without necessarily being exhaustive. While it is therefore obvious that additional trends could have been incorporated,[74] the working goal has been to ensure a high probability that the Internet & Jurisdiction Policy Network's stakeholders agree that all included trends are of significance.

---

72. Office of the Director of National Intelligence. (2017). *Global trends: Paradox of progress*. Retrieved from https://www.dni.gov/index.php/global-trends/near-future.

73. Internet & Jurisdiction Policy Network. *I&J Retrospect Database*. Retrieved from https://www.internetjurisdiction.net/publications/retrospect.

74. There are major trends, left out in this section, that are likely to become major jurisdictional issues within a foreseeable future. As pointed out by one interviewed expert, one such matter is found in that there is an increasing concern about digital labor issues. For example, persons employed to assess take-down request are becoming an integral part of the internet infrastructure doing menial tasks that greatly impact freedom of expression. Cross-border issues arise where such tasks are allocated to foreign workers, and questions have arisen as to the degree of support afforded to such workers who often are exposed to highly disturbing and offensive content. Issues such as this are important but have not been included in this year's Report.

3.1

Expression

The first category of major topical trends concerns expression. Recent discussions around the intersection of internet and jurisdiction and expression have focused on concerns about hate speech, extremism and fake news, as well as the widespread reform of data privacy regimes around the world. Increasingly broad claims pervade these discussions, and there is a growing appetite to re-examine the role of internet intermediaries.

Encouraging and facilitating cross-border expression has been a driving force behind much of the internet's development, both in physical (e.g., hardware) and non-physical (e.g., content platforms) dimensions. As many critical early developments originated in the US, the American perspective on freedom of speech – articulated in the First Amendment to the US Constitution – has colored much of the early discourse and guiding principles.[75] While weaker today due to the strong proliferation of internet usage outside the US – where more than 80% of Facebook's users now reside – the encouragement and facilitation of freedom of expression, including cross-border expression, remains a valued cornerstone of the internet in large parts of the world. In recognition of this, the UN has stressed that the right to freedom of expression on the internet is an issue of increasing importance.[76]

When asked what, if any, negative consequences they foresee if cross-border legal challenges on the internet are not properly addressed, 59% of surveyed experts raised the issue of potential restrictions on expression. This was one of the strongest concerns among the stakeholders.

Preliminary Table of Contents for Chapter 3.1

75. U.S. Const. amend. I. Retrieved from https://constitutioncenter.org/interactive-constitution/amendments/amendment-i.

76. See e.g.: United Nations, General Assembly. Human Rights Council: Draft Resolution: The promotion, protection and enjoyment of human rights on the internet, A/HRC/32/L.20 (June 27, 2016). Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement.

3.2

Security

The internet gives rise to numerous security issues, ranging from personal security to national security. As the internet continues to play an increasingly central role in society, internet security will only become more important. And in a world where more and more things are 'connected', it is becoming harder to separate online security from offline security.

The significance of this development is clearly reflected in the World Economic Forum's *Global Risks Report 2018*[77]. Among the Top 10 risks in terms of likelihood, 'cyberattacks' ranked 3rd and 'data fraud or theft' ranked 4th. This is particularly serious given that 'cyberattacks' is also ranked 6th among the top 10 risks in terms of impact.

This interconnectedness is palpable, as actions in one state impact other states, giving rise to many cross-border legal challenges in the context of security. These include:

- Countries may struggle to collaborate on, and coordinate, security efforts;
- Criminals may benefit significantly from jurisdictional obstacles to the detection, investigation and prosecution of their misdeeds;
- Ensuring access to digital evidence often depends on the cooperation of private actors, which has sparked a re-examination of the role they hold;
- States seeking to place their citizens under surveillance may need the voluntary or coerced cooperation of foreign privately-operated platforms, and breaking encryption may depend on the cooperation of foreign hardware manufacturers;
- Data breaches by a company in one state may impact a worldwide group of users; and
- States may adopt e-government solutions that involve storing critical data on servers in foreign countries.

It is also increasingly difficult to distinguish between the regulation of security and other fields of regulation. Security requirements, for example, are a standard aspect of many data privacy regimes. In that regard, data privacy and security are two sides of the same proverbial coin, even though the two are often portrayed in opposition to one another.

In the online security field, it is sometimes difficult to distinguish between civil wrongs, criminal offenses, acts of terrorism and even military aggression. This contributes to making regulation – and especially international consensus on regulatory responses – difficult to achieve.

But some distinctions are developing. In the context of access to digital evidence, for example, one interviewed expert noted that governments are increasingly emphasizing the need for different processes for national security matters compared to traditional criminal matters.

It is clear that the area of security is complex and multifaceted.

Preliminary Table of Contents for Chapter 3.2

77. World Economic Forum, The Global Risks Report 2018, 13th Edition. Retrieved from http://reports.weforum.org/global-risks-2018/.

3.3

Economy

In the economic context, much international attention has lately been directed at the cross-border application of territorially based intellectual property rights, taxation, and emerging technologies such as the Internet of Things and blockchain. As in the context of expression and security discussed above, the role of internet intermediaries is broadly being re-examined. In fact, with regard to the economy, there seems to be a more profound change in attitudes toward internet platforms.

Although it was not always the case, economical activities are now a natural and important part of the online environment. For example, it has been estimated that at least half of all trade in services is supplied via the internet;[78] and the World Economic Forum has estimated that the overall economic value of digital transformation to business and society will exceed 100 trillion US dollars by 2025.[79] Indeed, even when offered free of monetary charges, most online uses and activities are commercial to a significant extent.

The significance of the internet's economic dimension will continue to increase over the coming years, due to what has been termed Industry 4.0. That is:

"the next phase in the digitization of the manufacturing sector, driven by four disruptions: the astonishing rise in data volumes, computational power, and connectivity, especially new low-power wide-area networks; the emergence of analytics and business-intelligence capabilities; new forms of human-machine interaction such as touch interfaces and augmented-reality systems; and improvements in transferring digital instructions to the physical world, such as advanced robotics and 3-D printing."[80]

The digitalization of the economy – via access to an open internet and constant technological developments – is a driving force for growth. It enables companies, and particularly small and medium enterprises (SMEs), to compete on the world stage and create new opportunities in developing, ordering, producing, marketing or delivering their products and services. However, the ability to reach customers all over the globe at a faster pace and lower cost than ever before remains dependent upon a favorable regulatory environment.

"The ability to reach customers all over the globe at a faster pace and lower cost than ever before remains dependent upon a favorable regulatory environment."

Several surveyed and interviewed experts emphasized that complying with often complex laws from multiple sources calls for a degree of legal sophistication that is often beyond the reach of SMEs. Experts cited the complexity of privacy and consumer protection regulation and tax implications as specific examples. It was also noted that start-ups are exposed to the regulatory burden at a stage where they least can afford it. To build a user base, new businesses must often begin by giving away their services, before building a proven user base to secure revenue through advertisements. Yet the cost of ensuring regulatory compliance is incurred from the start – indeed, even prior to the launch of the service.

Experts also noted that SMEs are too often not part of regulatory discussions, which largely focus on the internet giants. At the same time, some experts pointed out that, compared to the large internet actors, SMEs are better placed to ignore claims of jurisdiction from distant states, as they can more easily avoid placing persons and assets within the reach of those states' enforcement powers.

69% of surveyed experts 'agreed', or 'strongly agreed', that the complexity of cross-border legal challenges on the internet is a significant barrier for SMEs entering the global digital economy. 21% 'neither agreed nor disagreed', and only 10% either 'disagreed', or 'strongly disagreed'.

---

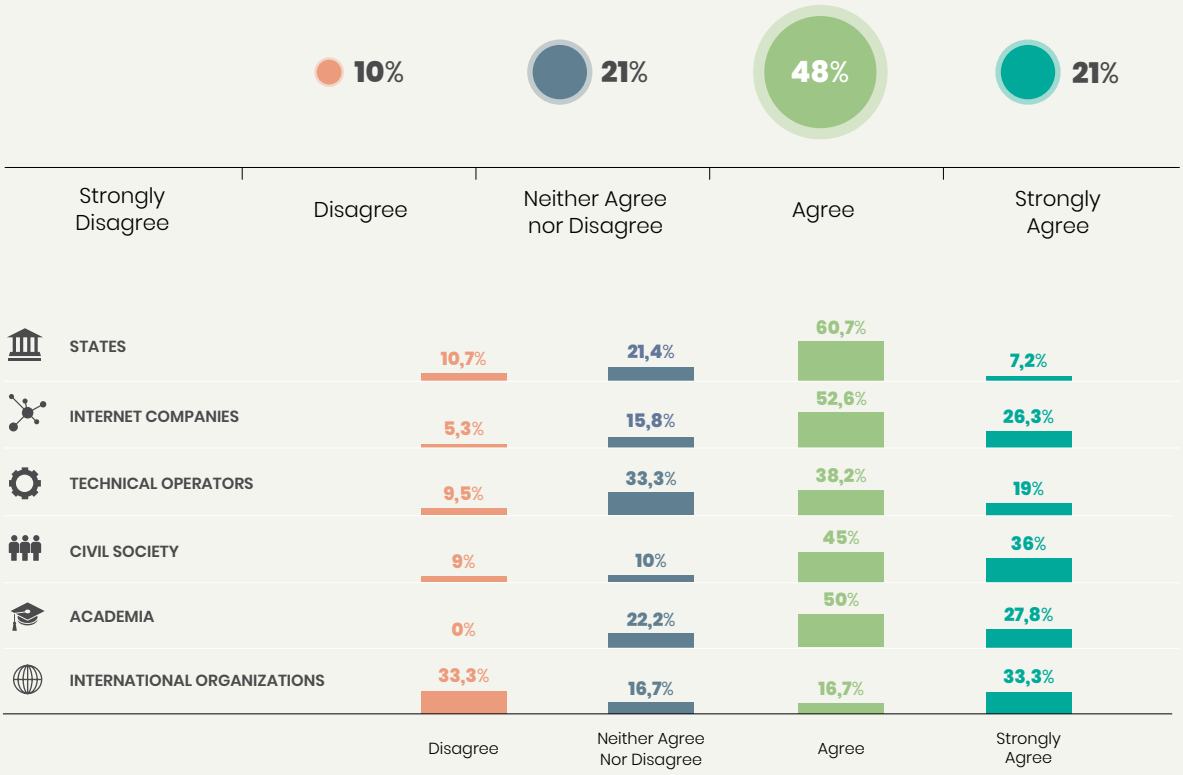
78. Lee-Makiyama. (2017, July 10). The digital trade oversight. *International Trade Forum.* Retrieved from http://www.tradeforum.org/article/The-digital-trade-oversight/.

79. Cann, O. (2016, January 22). $100 trillion by 2025: The digital dividend for society and business. *World Economic Forum.* Retrieved from https://www.weforum.org/press/2016/01/100-trillion-by-2025-the-digital-dividend-for-society-and-business/.

80. Baur, C. & Wee, D. (2015 June). Manufacturing's next act. *McKinsey & Company*. Retrieved from https://www.mckinsey.com/business-functions/operations/our-insights/manufacturings-next-act.

INFOGRAPHIC 13

Are cross-border legal challenges on the internet a significant barrier for Small and Medium Enterprises (SMEs)?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

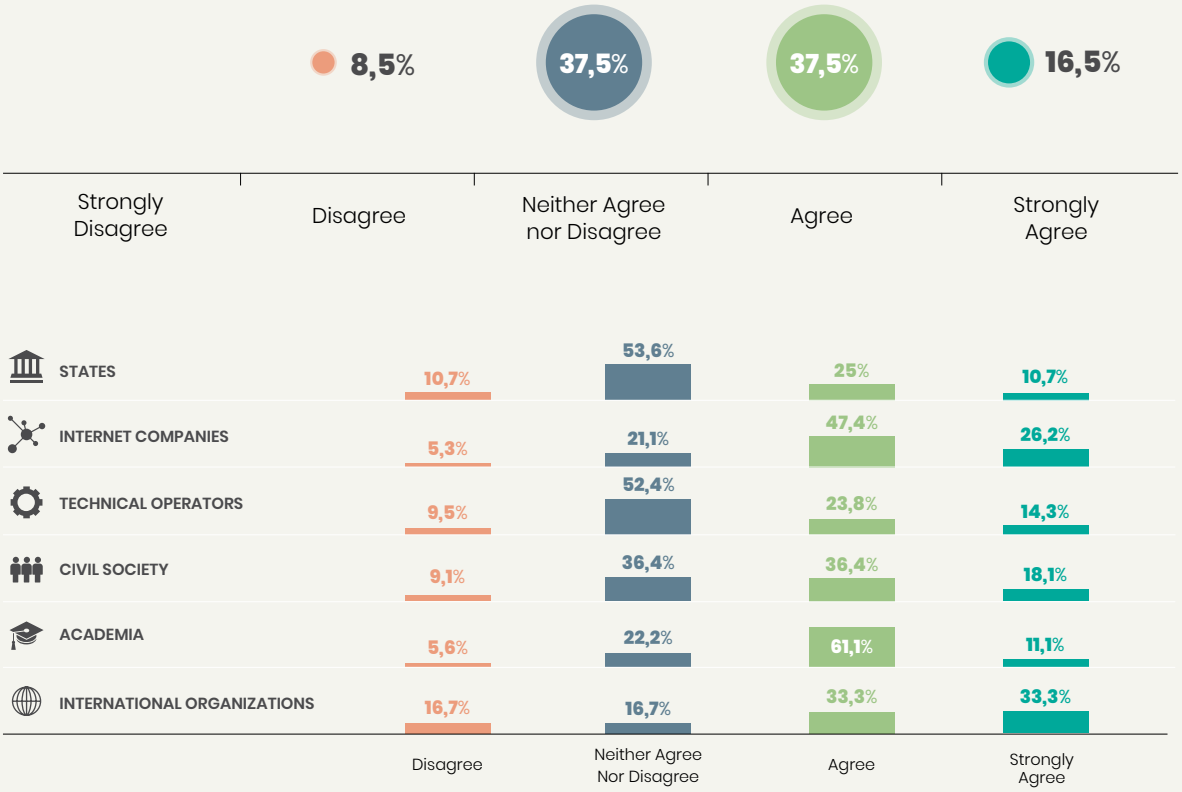
These figures were largely consistent across the different regions and stakeholder groups. Some, however, asserted that the complexity of cross-border legal challenges on the internet is not so much a barrier for SMEs entering the global digital economy, as it is a barrier for SMEs seeking growth in the global digital economy. Cross-border trade on the internet also has the potential to be an equalizer between the developed and developing world, as it allows developing countries to bypass some of the steps today's developed countries had to go through. Yet while the potential advantages are great, so are some of the obstacles.

In the survey study, 54% of surveyed experts 'agreed', or 'strongly agreed', that the complexity of cross-border legal challenges on the internet is a significant barrier for developing countries entering the global digital economy. 37,5% 'neither agreed nor disagreed', and only 18,5% either 'disagreed', or 'strongly disagreed', that the complexity of cross-border legal challenges on the internet is a significant barrier for developing countries entering the global digital economy.

> "Cross-border trade on the internet also has the potential to be an equalizer between the developed and developing world."

INFOGRAPHIC 14

Are cross-border legal challenges on the internet a significant barrier for developing countries?



SOURCE: Internet & Jurisdiction Policy Network: Internet & Jurisdiction Global Status Report 2019

One surveyed expert noted that even the fear of the legal difficulties associated with cross-border internet activity dissuades people in developing countries from engaging in such activities. Further, one interviewed expert noted that the main difficulty facing developing countries is the significantly faster pace at which the internet evolves today, compared to the past. The pace of change in the regulatory environment and its complexification – due, in large part, to an increased regulatory appetite and extraterritoriality – is increasing, as well. Yet the survey also revealed a marked difference in attitudes among surveyed experts from different regions and their comments provide an explanation for these strong regional differences. Both surveyed and interviewed experts emphasized that poverty, skill levels, illiteracy, language barriers, political instability, lack of investors and poor ICT infrastructure are bigger concerns in regions such as Africa and some parts of Latin America, than are the legal cross-border challenges.

Experts also raised the point that developing countries are often not part of, and indeed not even aware of, agreements and other regulatory developments discussed or concluded among developed countries. Experts observed that developing countries experience difficulties when developed countries seek to apply their laws in an extraterritorial manner that affects developing countries, including businesses and persons in developing countries. There is also a perception that, compared to developed countries, developing countries have less of a say in the approaches taken by major internet actors. This sense of disempowerment is a clear

trend, and arguably pressures developing countries to choose between existing, partially competing approaches (e.g., between a 'Western approach' promoting democratic values and a Chinese 'digital sovereignty' approach) rather than having the opportunity to develop their own approaches.

Surveyed and interviewed experts also observed that much of the online activity in developing countries is local in nature, and therefore confronts the complexity of cross-border legal challenges on the internet less often.

Taken together, this suggests that although the complexity of cross-border legal challenges on the internet is an important barrier for developing countries entering the global digital economy, it is just one of several – and perhaps not the most acute.

Preliminary Table of Contents for Chapter 3.3

04

LEGAL AND TECHNICAL APPROACHES

PREVIEW

After a long period of relative inaction, there are now myriad legal approaches to addressing the cross-border legal challenges on the internet. Particularly over the past five years, both developing and industrialized countries have stopped procrastinating and taken a multiplicity of uncoordinated actions.

Some jurisdictions have advanced with remarkable speed, setting global norms that compete, at least in part, with global norm-setting initiatives of other jurisdictions. Indeed, it may not be an exaggeration to speak of an ongoing race toward global norm setting between the EU, the US, China and, to a lesser extent, Russia.

States seek competitive advantages in this race in a variety of ways, ranging from political initiatives, such as building capacity, and creating financial and security dependence among other countries, to the use of legal tools such as extraterritoriality and treaties. In this landscape, there is now a clear distinction between jurisdictions that set norms, and those that largely adopt the norms set by others. Unsurprisingly, smaller and developing countries are almost exclusively on the receiving end. Although laws offer some solutions, there is recognition that public-private standards or industry self-regulation may offer solutions, as well.

> "Over the past five years, both developing and industrialized countries have stopped procrastinating and taken a multiplicity of uncoordinated actions."

Several technical solutions have been advanced, each with a substantial impact on the cross-border legal challenges on the internet. The aforementioned race toward global norm setting is playing out in this context, as well, with measures such as internet shutdowns, blocking and the forceful acquisition of innovation enablers making headlines in the news.

This Chapter outlines and analyzes a selection of major legal and technical approaches to solutions that experts emphasized in surveys and interviews, or that have gained particularly strong attention in the literature.

As one interviewed expert noted, the fact that the issues with which stakeholders now struggle are not new can either be viewed as a source of reassurance, or a cause for concern.

4.1 Major legal approaches to solutions

States take a wide range of legal approaches in the pursuit of what they perceive to be solutions to the cross-border legal challenges on the Internet. There is clearly an increased appetite for so-called 'takedown' and 'stay-down' orders from courts. There are also signs of a race to the highest potential fines – states are increasing the penalties they impose in order to

prioritize adherence to their particular laws (over the adherence to competing legal frameworks imposed by other states).

Another emerging tool used to ensure enforceability of state law is so-called 'rep localization' – that is, laws requiring businesses to nominate a local representative within the state imposing the requirement. In addition, states are increasingly engaging in what may be described as jurisdictional trawling, whereby they make excessively broad claims of jurisdiction, giving them considerable discretion in deciding whom to direct their enforcement efforts against. There is also a persistent, and perhaps growing, reliance on jurisdictional tests focused on 'targeting'.

At the same time, however, there are some signs of restraint. While it remains a contested concept on the international level, comity and other calls for interest balancing are discernable on several levels. Furthermore, the matter of how states approach the scope of jurisdiction still hangs in the balance. Will the emerging practice of states seeking to give their judgments global effect become cemented? Or will a more nuanced approach prevail? This will be a key battleground in the coming years.

Finally, the extent to which terms of service and community guidelines, rather than law, shape online behavior remains a live issue.

As discussed in the Introduction, attempts at finding legal approaches to solving the cross-border legal issues facing the internet are hampered by 'artificial regulatory challenges' – that is, contemporary frameworks and concepts are insufficient to successfully address these issues.

Overcoming such artificial regulatory challenges may require changes to traditional frameworks and concepts. But it also requires capacity building, which dovetails with the need for inclusiveness – a key issue to be considered in the context of approaches to solutions, and a recurring theme cited by surveyed and interviewed experts.

Both developing countries and many smaller states around the world are seen to be in the position of 'price-takers' – i.e., they must accept prevailing solutions and approaches from larger countries, without providing meaningful input. One interviewed expert suggested that this leads to a feeling of technological colonization, which causes particular resentment in countries with a colonial history.

While this point is raised in various contexts throughout the Report, it should certainly be considered in the examination of current approaches to solutions. It is important to assess not only how well these approaches work in the countries at the forefront of internet technologies, but how they impact developing and smaller countries, as well. Further, it is not enough to consider how well these approaches to solutions work today. It is also necessary to consider how they will work in the future, when the online environment is even more diverse.

Preliminary Table of Contents for Chapter 4.1

4.2

Major technical approaches to solutions

Many of the legal issues that arise in the context of internet technology may also be solved through that same technology. This section describes and examines the role of particularly significant technical approaches to solutions impacting the cross-border legal challenges on the internet. A theme uniting many of these technical approaches is that they focus on limiting access to content.

The first technical approach to solutions – the use of so-called geo-location technologies – is currently a major 'battle ground'. The survey carried out for this Report sheds light on a divergence of views on geo-location technologies among the Internet & Jurisdiction Policy Network's stakeholders. Other technical measures aimed at limiting access to content include:

- Content filtering on the national network level;
- Court ordered suspension, deletion, non-resolving, seizure and transfer in the context of the Domain Name System;
- Court ordered DNS blocking, IP Address blocking or re-routing and URL blocking in the context of the Domain Name System;
- Service shutdowns; and
- Internet shutdowns.

All these technical blocking measurers, at least in their current form, have the potential to be undermined, if not rendered useless, by the development of satellite-based internet connectivity such as the OneWeb[81] project and Iridium[82], which provide satellite-based broadband connectivity worldwide.

The trend of forced data localization requirements is also examined, and attention is given to the multifaceted impact of artificial intelligence.

Technological complexity poses an obstacle to finding useful technical approaches to solutions to the cross-border legal challenges on the internet. Therefore, as in the context of legal approaches to solutions, there is a need for capacity building on every level. Technical capacity building is needed among both internet users and SMEs, as well as administrators, law enforcement, courts, governments and other stakeholders. This need is particularly acute in developing countries, but it also exists at the highest levels in developed countries.[83]

Preliminary Table of Contents for Chapter 4.2

81. https://www.oneweb.world/.
82. https://www.iridium.com/.
83. See e.g.: Farrell, H. (2018, December 5). Rudy Giuliani is Trump's cybersecurity adviser. He might want a refresher. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/monkey-cage/wp/2018/12/05/rudy-giuliani-is-trumps-cybersecurity-adviser-he-might-want-a-refresher/?noredirect=on&utm_term=.603492432f39, and BBC News. (2018, November 15). *Japan's cyber-security minister has 'never used a computer'*. Retrieved from https://www.bbc.com/news/technology-46222026.

05

RELEVANT CONCEPT CLUSTERS

—

PREVIEW

As noted in the Introduction, and as observed by interviewed and surveyed experts, progress on the cross-border legal challenges faced on the internet has been hindered, in part, by the insufficiency of the framework and concepts we use to address these challenges. The entire field suffers from an 'artificial regulatory challenge'.

The conceptual complexity prevents informed participation for many stakeholders, and frequently results in misunderstanding and miscommunication. Many concepts must be agreed upon (and understood) in order to foster a productive discussion of the cross-border legal challenges faced on the internet. Complicating matters further is the fact that these concepts are often only properly understood when viewed in relation to other related concepts.

This section of the Report will highlight various relevant 'concept clusters', with the aim to both discuss a selection of concepts and illustrate how they relate to one another. Some key concepts – such as the concept of 'jurisdiction' – must be viewed in relation to several other concepts, and are thus discussed as part of several clusters.

Preliminary Table of Contents for Chapter 5


INTERNET &
JURISDICTION
POLICY NETWORK

The Internet & Jurisdiction Policy Network is the multistakeholder organization addressing the tension between the cross-border nature of the internet and national jurisdictions.

Its Secretariat facilitates a global policy process between key stakeholders to enable transnational cooperation and policy coherence. Participants in the Policy Network work together to preserve the cross-border nature of the Internet, protect human rights, fight abuses, and enable the global digital economy. Since 2012, the Internet & Jurisdiction Policy Network has engaged more than 200 key entities from different stakeholder groups around the world, including governments, the world's largest Internet companies, the technical community, civil society groups, leading universities and international organizations.